

**Generalny Inspektor  
Ochrony Danych Osobowych**

**SPRAWOZDANIE  
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA  
OCHRONY DANYCH OSOBOWYCH  
W ROKU 2012**

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zgodnie z którym Generalny Inspektor Ochrony Danych Osobowych składa Sejmowi, raz w roku, sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych<sup>1</sup>.

---

<sup>1</sup> Niniejsze *Sprawozdanie* obejmuje okres działalności Generalnego Inspektora Ochrony Danych Osobowych od 1 stycznia 2012 r. do 31 grudnia 2012 r.

## SPIS TREŚCI

<b>WPROWADZENIE .....</b>	<b>5</b>
<b>CZĘŚĆ I. PRAWNE PODSTAWY DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH .....</b>	<b>6</b>
1. INFORMACJE OGÓLNE.....	6
2. REFORMA OCHRONY DANYCH OSOBOWYCH W UNII EUROPEJSKIEJ .....	9
3. BIURO GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH.....	11
3.1. <i>Struktura organizacyjna .....</i>	<i>11</i>
3.2. <i>Pracownicy Biura GODO .....</i>	<i>12</i>
3.3. <i>Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2012 rok..13</i>	<i>13</i>
<b>CZĘŚĆ II. STAN WIEDZY I PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH.....</b>	<b>14</b>
1. INFORMACJE OGÓLNE.....	14
2. KONTROLA ZGODNOŚCI PRZETWARZANIA DANYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH .....	16
2.1. <i>Czynności kontrolne.....</i>	<i>16</i>
2.2. <i>Kontrola przetwarzania danych osobowych w wybranych obszarach .....</i>	<i>17</i>
2.2.1. Administracja publiczna .....	17
2.2.2. Bezpieczeństwo publiczne.....	18
2.2.3. Banki i inne instytucje finansowe.....	22
2.2.4. Telekomunikacja.....	25
2.2.5. Zatrudnienie .....	28
2.2.6. Służba zdrowia .....	30
2.2.7. Szkolnictwo wyższe.....	41
2.2.8. Usługi hotelarskie .....	45
2.2.9. Inne .....	47
2.3. <i>Systemy informatyczne służące do przetwarzania danych osobowych .....</i>	<i>52</i>
2.4. <i>Wyniki kontroli w zakresie wypełnienia obowiązków formalnych i organizacyjnych .....</i>	<i>54</i>
2.5. <i>Wyniki kontroli w zakresie warunków techniczno-organizacyjnych.....</i>	<i>56</i>
3. WYDAWANIE DECYZJI ADMINISTRACYJNYCH I ROZPATRYWANIE SKARG W SPRAWACH WYKONANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH .....	60
3.1. <i>Wydawanie decyzji.....</i>	<i>60</i>
3.2. <i>Zawiadomienia o podejrzeniu popełnienia przestępstwa .....</i>	<i>61</i>
3.3. <i>Rozpatrywanie skarg .....</i>	<i>65</i>

4.	EGZEKOWANIE OBOWIĄZKÓW O CHARAKTERZE NIEPIENIĘŻNYM OKREŚLONYCH W DECYZJACH ADMINISTRACYJNYCH GIDO .....	95
5.	PROWADZENIE REJESTRU ZBIORÓW DANYCH ORAZ UDZIELANIE INFORMACJI O ZAREJESTROWANYCH ZBIORACH .....	100
6.	OPINIOWANIE PROJEKTÓW USTAW I ROZPORZĄDZEŃ DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH .....	114
7.	INICJOWANIE I PODEJMOWANIE PRZEDSIĘWZIĘĆ W ZAKRESIE DOSKONALENIA OCHRONY DANYCH OSOBOWYCH .....	176
7.1.	<i>Interpretacja przepisów</i> .....	177
7.1.1.	Podmioty świadczące usługi z zakresu ochrony zdrowia .....	178
7.1.2.	Banki i inne instytucje finansowe oraz firmy windykacyjne.....	183
7.1.3.	Przetwarzanie danych osobowych – wybrane problemy .....	191
7.1.4.	Wystąpienia .....	207
7.2.	<i>Działalność informacyjna</i> .....	227
7.2.1.	Współpraca ze środkami masowego przekazu .....	228
7.2.2.	Publikacje .....	232
7.2.3.	Dni Otwarte Generalnego Inspektora Ochrony Danych Osobowych.....	233
7.2.4.	Szkolenia .....	235
7.2.5.	Konkursy .....	238
7.2.6.	Projekty i programy .....	239
7.2.7.	Konferencje, seminaria, spotkania.....	244
7.2.8.	Porozumienia o współpracy.....	260
7.2.9.	Inne informacje.....	261
8.	UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ PROBLEMATYKĄ OCHRONY DANYCH OSOBOWYCH.....	262
8.1.	<i>Międzynarodowe konferencje, seminaria i spotkania</i> .....	275
8.2.	<i>Wizyty robocze</i> .....	280
8.3.	<i>Międzynarodowe warsztaty</i> .....	281
<b>CZĘŚĆ III. CHARAKTERYSTYKA DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W 2012 ROKU .....</b>		<b>283</b>
<b>CZĘŚĆ IV. WNIOSKI I PLANOWANE KIERUNKI DZIAŁAŃ GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH.....</b>		<b>314</b>

## **Załączniki**

<b>Załącznik nr 1</b>	Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2012 o charakterze generalnym do centralnych organów państwa i do innych podmiotów sektora publicznego .....	327
<b>Załącznik nr 2</b>	Wykaz kontroli przeprowadzonych w 2012 roku .....	329
<b>Załącznik nr 3</b>	Wykaz orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie i Naczelnego Sądu Administracyjnego wydanych w 2012 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych .....	335
<b>Załącznik nr 4</b>	Informacje przekazane przez organy ścigania w sprawach skierowanych w 2012 roku przez Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o popełnieniu przestępstwa .....	340
<b>Załącznik nr 5</b>	Wykaz szkoleń przeprowadzonych przez GODO w 2012 r. ....	341
<b>Załącznik nr 6</b>	Wykaz wydarzeń objętych patronatem GODO w 2012 r. ....	344
<b>Załącznik nr 7</b>	Wykaz konferencji, seminariów i spotkań krajowych i międzynarodowych z udziałem GODO lub jego przedstawicieli, zorganizowanych w 2012 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty .....	346
<b>Załącznik nr 8</b>	Wykaz konferencji, seminariów i spotkań międzynarodowych z udziałem GODO lub jego przedstawicieli, które odbyły się w 2012 r. za granicą .....	352
<b>Załącznik nr 9</b>	Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych wydanych w 2012 r. w sprawach o wyrażenie zgody na przekazanie danych osobowych za granicę .....	356

# **SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2012**

## **Wprowadzenie**

Prawo do ochrony danych osobowych ustanowione jest w art. 8 Karty praw podstawowych Unii Europejskiej, w którym zapisano ochronę danych osobowych jako jedno z praw podstawowych, oraz w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), który ustanawiał zasadę, zgodnie z którą każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo do ochrony danych osobowych nie jest prawem absolutnym i powinno być analizowane w kontekście funkcji, jaką pełni w społeczeństwie. Ochrona danych osobowych jest bowiem ściśle powiązana z poszanowaniem życia prywatnego i rodzinnego chronionego na podstawie art. 7 Karty.

Podstawowy dokument ustanawiający obowiązujące unijne przepisy o ochronie danych osobowych – **dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych** (Dz. U. L. 281 z 23.11.1995 r.) – został przyjęty z myślą o realizacji dwóch celów: ochrony podstawowych praw i wolności osób fizycznych, a w szczególności ich prawa do prywatności w kontekście przetwarzania danych osobowych oraz zagwarantowania swobodnego przepływu danych między państwami członkowskimi. Powyższa dyrektywa została uzupełniona przez decyzję ramową 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. U. L 350 z 30.12.2008 r.). Zakres stosowania tej decyzji jest ograniczony do przetwarzania danych osobowych przekazywanych lub udostępnianych pomiędzy państwami członkowskimi w obszarze dawnego trzeciego filaru UE.

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.) stanowiła implementację ww. dyrektywy do polskiego porządku prawnego, przyczyniając się w ten sposób do stworzenia systemu ochrony danych osobowych w Polsce. Istotnym elementem tego systemu - oprócz ww. ustawy – były przede wszystkim normy konstytucyjne: Art. 47 – gwarantujący obywatelom prawo do prywatności oraz Art. 51 gwarantujący każdemu prawo do ochrony informacji dotyczących jego osoby. Wprowadzenie przepisów dotyczących ochrony danych osobowych do polskiego systemu prawnego pozwoliło także na podpisanie przez Polskę w dniu 21 kwietnia 1999 r. i następnie ratyfikowanie w dniu 24 maja 2002 r. - Konwencji Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych.

Zadania i kompetencje Generalnego Inspektora Ochrony Danych Osobowych wyznaczają przepisy ww. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. W ich świetle GODO 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**

Generalny Inspektor Ochrony Danych Osobowych jest jednoosobowym organem administracji publicznej, który wykonuje ustawowe zadania przy pomocy Biura. Działaniem swym obejmuje sektor

publiczny i prywatny. Jego kompetencje obejmują nadzór i kontrolę przestrzegania przepisów o ochronie danych osobowych, prowadzenie rejestru zbiorów danych osobowych, rozpatrywanie skarg i wydawanie decyzji administracyjnych, zapewnienie wykonania przez zobowiązanych obowiązków wynikających z decyzji organu przez stosowanie środków egzekucyjnych, udzielanie porad prawnych i konsultacji z zakresu ochrony danych osobowych, rozpowszechnianie informacji z zakresu ochrony danych osobowych oraz współpraca międzynarodowa. Generalny Inspektor Ochrony Danych Osobowych jest odpowiedzialny za wdrażanie prawa w zakresie ochrony danych osobowych i nadzór nad realizacją ustawy o ochronie danych osobowych i w tym zakresie współpracuje z krajowymi podmiotami oraz innymi europejskimi i pozaeuropejskimi organami ochrony danych osobowych oraz instytucjami zajmującymi się szeroko rozumianymi prawami człowieka.

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) i rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2011 r. Nr 103, poz. 601) – 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).

Od 1 stycznia 2012 r. zaczęły obowiązywać nowe przepisy prawa mające istotny wpływ na ochronę danych osobowych. W tym dniu weszła w życie ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz. U. Nr 230, poz. 1371), która w dużym stopniu wdrożyła w polskim porządku prawnym decyzję ramową 2008/977/WSiSW, jak również wprowadziła zmiany w treści art. 26a, art. 43 i art. 47 ustawy o ochronie danych osobowych<sup>2</sup>.

Ponadto, z dniem 31 grudnia 2011 r. stracił moc obowiązującą art. 7a ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej, który stanowił, że „Ewidencja działalności gospodarczej jest jawna i dane osobowe w niej zawarte nie podlegają przepisom ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych”. Oznacza to, że od 1 stycznia 2012 r. przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych dotyczą informacji identyfikujących przedsiębiorców w obrocie gospodarczym, o ile – dla konkretnego stanu faktycznego – będą stanowiły dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych. Tym samym administratorzy danych osobowych dotyczących przedsiębiorców będą musieli wypełnić wszelkie obowiązki wynikające z ustawy o ochronie danych osobowych, w tym te dotyczące rejestracji zbiorów danych osobowych.

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.

---

<sup>2</sup> Porównanie dotychczas obowiązujących przepisów ustawy o ochronie danych osobowych z ich obecnym brzmieniem po nowelizacji zaprezentowane jest formie tabelki na stronie internetowej: [http://www.giodo.gov.pl/560/id\\_art/4474/j/pl/](http://www.giodo.gov.pl/560/id_art/4474/j/pl/).



## 2. Reforma ochrony danych osobowych w Unii Europejskiej

Ważnym wydarzeniem z perspektywy organu ds. ochrony danych osobowych, było przedstawienie przez Komisję Europejską w dniu 25 stycznia 2012 r. pakietu dotyczącego reformy ochrony danych osobowych w Unii Europejskiej, w oparciu o który Rada UE i Parlament Europejski rozpoczęły realizację odpowiednich procedur w ramach procesu legislacyjnego.

Unijna reforma prawa o ochronie danych zakłada 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 pozalegisacyjnych mających na celu skuteczniejszą ochronę danych osobowych w Unii Europejskiej (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.

Pakiet zmian regulacji UE w zakresie ochrony danych osobowych przewiduje 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 (tzw. ogólne rozporządzenie o ochronie danych)**<sup>3</sup>. Rozporządzenie to co do zasady obowiązywać będzie 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 i swobodny przepływ 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 ich i ścigania lub wykonywania sankcji karnych i swobodnego przepływu tych danych**<sup>4</sup>, której zasady nie znajdują w tak szerokim zakresie odbicia w obowiązujących obecnie przepisach polskiego prawa<sup>5</sup>.

---

<sup>3</sup> Wniosek Komisji Europejskiej COM (2012) 11 final

<sup>4</sup> Wniosek Komisji Europejskiej COM (2012) 10 final

<sup>5</sup> Podkreślenia wymaga, że zakres zastosowania decyzji ramowej 2008/977/WSiSW, jak i implementującej ją do polskiego porządku prawnego ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz. U. Nr 230, poz. 1371), jest ograniczony do danych osobowych przetwarzanych w ramach współpracy transgranicznej.

Przedstawienie przez Komisję Europejską pakietu zmian regulacji UE w zakresie ochrony danych osobowych odbyło się w dniu 25 stycznia 2012 r. w Brukseli. Parlament Europejski wyznaczył Komisję ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) na główną komisję odpowiedzialną za oba wnioski, której zadaniem było przedstawienie projektów opinii na ich temat. Podczas 14. Spotkania Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA) w maju 2012 r. w którym uczestniczył Generalny Inspektor Ochrony Danych Osobowych, Rzecznicy zadeklarowali poparcie dla europejskiej reformy ochrony danych i wyrazili gotowość kontynuowania współpracy w celu doprowadzenia do kompleksowej modernizacji europejskich ram ochrony danych w taki sposób, aby miały zastosowanie we wszystkich obszarach. Akceptując propozycje kompleksowej reformy ram prawnych ochrony danych osobowych Unii Europejskiej przedstawionych przez Komisję Europejską, mających na celu wzmocnienie praw osób fizycznych oraz sprostanie wyzwaniom globalizacji i nowych technologii, jak również propozycję modernizacji Konwencji Nr 108 Rady Europy, Europejscy Rzecznicy Ochrony Danych z uznaniem przyjęli zaproponowane także w nowych przepisach rozwiązanie kwestii rozliczalności administratorów danych i przetwarzających, zmniejszenie niektórych obciążeń administracyjnych i dążenie do ich spójności oraz przypisanie kluczowej roli organom ochrony danych poprzez wzmocnienie ich niezależności i uprawnień.

Natomiast polski organ ds. ochrony danych osobowych podjął szereg działań na szczeblu krajowym (konferencje, seminaria, konsultacje), aby informacje na temat proponowanych regulacji prawnych dotyczących obrotu informacją w UE przeniknęły do świadomości społecznej. Zagadnienia nowych ram prawnych ochrony danych osobowych pozostawały bowiem wysoko na liście priorytetów działalności GIODO w 2012 r.

W dniu 16 lutego 2012 r. Komisja Sprawiedliwości i Praw Człowieka Sejmu RP wysłuchiwała informacji na ten temat przedstawionych przez dra Wojciecha R. Wiewiórowskiego, GIODO, a następnie przedyskutowane zostały kwestie relacji pomiędzy przepisami krajowymi a unijnymi w tym zakresie oraz problem rejestracji zbiorów danych, w tym dotyczących kościołów i związków wyznaniowych. W dniu 7 marca 2012 r. Generalny Inspektor Ochrony Danych Osobowych wspólnie z Komisją Europejską oraz Krajową Szkołą Administracji Publicznej zorganizował w Warszawie konferencję pt. „Reforma regulacji ochrony danych osobowych w Unii Europejskiej. Wstępna ocena jej zakresu i konsekwencji”, która zapoczątkowała szeroką dyskusję poświęconą planom ukształtowania nowego modelu ochrony prywatności i danych osobowych w Unii Europejskiej. W jej rezultacie GIODO odbył także szereg spotkań i konsultacji z różnymi podmiotami krajowymi, zainteresowanymi tym zagadnieniem. Wśród nich znaleźli się przedstawiciele sektora telekomunikacji i IT zrzeszonych w Polskiej Izbie Informatyki i Telekomunikacji, środowiska bankowego (Związku Banków Polskich, Biura Informacji Kredytowej), prawniczego – w tym Krajowej Rady Sądowniczej, Polskiej Izby

Ubezpieczeń oraz Polskiej Organizacji Handlu i Dystrybucji. Waga sygnalizowanych przez te podmioty kwestii okazała się bardzo znacząca w kontekście dalszych prac nad unijnym projektem oraz planowanych zmian w polskich przepisach prawa o ochronie danych osobowych.

W 2012 r. GODO zainicjował także serię wewnętrznych spotkań z pracownikami Biura GODO, podczas których omawiane było stanowisko polskiego organu wobec proponowanych zmian oraz ustalane były kwestie wymagające dalszej pracy, jeśli chodzi o przyszłość polskiego prawa o ochronie danych osobowych i jego interpretacji.

### **3. Biuro Generalnego Inspektora Ochrony Danych Osobowych**

#### **3.1. Struktura organizacyjna**

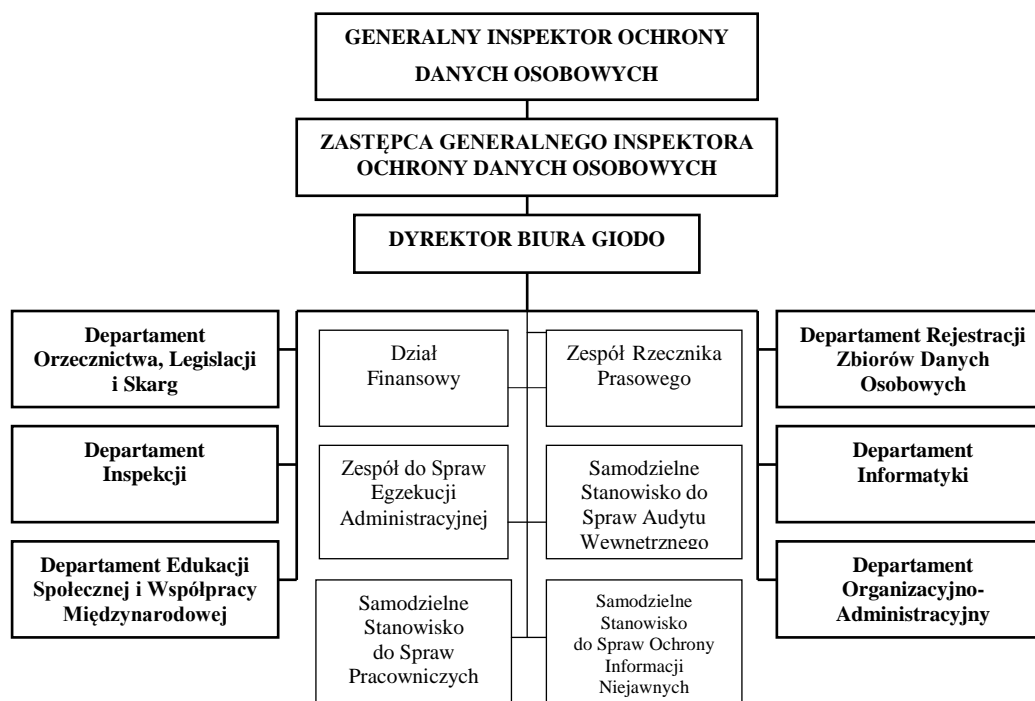
Zgodnie z art. 13 ust. 1 ustawy o ochronie danych osobowych, Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. W przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie, może wykonywać swoje zadania 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 GODO – 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

Generalny Inspektor wykonuje swoje zadania bezpośrednio lub przy pomocy Dyrektora Biura, dyrektorów jednostek organizacyjnych Biura oraz innych osób wskazanych w Regulaminie Organizacyjnym<sup>6</sup>.

### 3.2. Pracownicy Biura GODO

Stan zatrudnienia w Biurze GODO w przeliczeniu na pełne etaty wynosił na dzień 1 stycznia 2012 r. – 126,48 etatów, zaś na dzień 31 grudnia 2012 r. – 124,48 etatów. Na stanowiskach merytorycznych zatrudnionych było 112 osób, a na stanowiskach pomocniczych 16 osób. Wyższe wykształcenie posiadało 110 pracowników, w tym 71 legitymowało się wykształceniem wyższym prawniczym.

<sup>6</sup> 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.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2012 r. przedstawia się następująco:

- GIODO - 1 osoba
- Zastępca GIODO – 1 osoba
- Dyrektor Biura – 1 osoba
- Zespół Rzecznika Prasowego (ZRP) – 5 osób (5 etatów)
- Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) – 9 osób (8,75 etatu),
- Departament Informatyki (DIF) – 15 osób (15 etatów),
- Departament Inspekcji (DIS) – 15 osób (15 etatów),
- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 32 osoby (32 etaty),
- Departament Rejestracji Zbiorów Danych Osobowych (DRZDO) – 17 osób (17 etatów),
- Departament Organizacyjno-Administracyjny (DOA) – 18 osób (16,4 etatu),
- Dział Finansowy – 3 osoby (3 etaty),
- Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,5 etatu),
- Samodzielne Stanowisko ds. Pracowniczych – 2 osoby (1,5 etatu),
- Samodzielne Stanowisko ds. Audytu – 1 osoba (0,33 etatu),
- Radcy Prawni – 3 osoby (2 etaty),
- Zespół ds. Egzekucji Administracyjnej (ZEA) – 3 osoby (3 etaty).

W nowym Regulaminie Organizacyjnym Biura Generalnego Inspektora Ochrony Danych Osobowych stanowiącym załącznik nr 1 do Zarządzenia Nr 1/2012, który wszedł w życie z dniem 4 stycznia 2012 r.<sup>7</sup>, została wyodrębniona nowa jednostka organizacyjna – Zespół do Spraw Egzekucji Administracyjnej (ZEA).

### **3.3. Wykonanie budżetu Generalnego Inspektora Ochrony Danych Osobowych za 2012 rok**

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2012 r. wynosił: **15 060** tys. zł, w tym:

- wynagrodzenia	9 355 tys. zł
- pochodnie od wynagrodzeń	1 564 tys. zł
- wydatki majątkowe	409 tys. zł
- pozostałe wydatki	3 732 tys. zł

---

<sup>7</sup> 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.

Wydatki zrealizowane przez GIODO w 2012 roku w kwocie **14 520** tys. zł obejmowały:

- wynagrodzenia	9 020 tys. zł
- pochodne od wynagrodzeń	1 504 tys. zł
- wydatki majątkowe	394 tys. zł
- pozostałe wydatki	3 602 tys. zł

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

### **1. Informacje ogólne**

Każdy ma prawo do ochrony dotyczących go danych osobowych. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych wprowadza szczegółowe normy służące realizacji tego prawa. W szczególności reguluje postępowanie przy przetwarzaniu danych osobowych, czyli operacjach takich, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą. Za dane osobowe uważa się wszelkie informacje dotyczące osoby fizycznej, pozwalające bez większego wysiłku na określenie tożsamości tej osoby. Danymi osobowymi nie będą jednak pojedyncze informacje o dużym stopniu ogólności. Staną się nimi dopiero z chwilą zestawienia ich z innymi, dodatkowymi informacjami, które w konsekwencji pozwolą na odniesienie ich do konkretnej osoby.

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

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 26 ust. 1 ustawy, ujmując je w formę podstawowych obowiązków administratora danych<sup>8</sup>. Z jego treści wynika, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, ma on przestrzegać wskazanych poniżej zasad:

- 1) legalności – dane mogą być przetwarzane tylko na podstawie przepisów prawa,
- 2) celowości – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z tymi celami,

---

<sup>8</sup> Administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych (art. 7 pkt 4 ustawy o ochronie danych osobowych). Między innymi może to być organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna.

- 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 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 osobowych, 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 ten 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 lub innego przewidzianego prawem przeciwko osobom winnym dopuszczenia do uchybień.

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

W 2012 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **165 kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych.

### **2.2.1. Administracja publiczna**

W 2012 r. inspektorzy Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili **8 kontroli w podmiotach z sektora administracji publicznej** – w Ministerstwie Pracy i Polityki Społecznej, w Wojewódzkim Urzędzie Pracy, Powiatowych Urzędach Pracy, w urzędach miejskich, w Miejskim Ośrodku Pomocy Społecznej oraz w Miejskich Ośrodkach Pomocy Rodzinie.

Do jednej z bardziej interesujących kontroli przeprowadzonych w 2012 r. należała kontrola jednego z powiatowych urzędów pracy (PUP). W jej toku ustalono, iż pracownicy miejskich ośrodków pomocy społecznej (MOPS), jak również pracownicy miejskich ośrodków pomocy rodzinie (MOPR) - działających na terenie obsługiwanych przez PUP, poprzez dedykowany system informatyczny mieli dostęp do danych osób bezrobotnych i osób poszukujących pracy (tj. klientów PUP) - do pozyskiwania których są uprawnieni na podstawie przepisów prawa. Ustalono również, iż pracownicy ww. jednostek za pomocą przedmiotowego systemu mieli także dostęp do danych klientów powiatowego urzędu

pracy, do pozyskania których nie uprawniają ich przepisy, gdyż osoby, których dane dotyczą nie ubiegają się o żadne świadczenia przyznawane przez te jednostki. Biorąc powyższe pod uwagę Generalny Inspektor stwierdził, iż udostępnianie przez PUP (za pomocą ww. systemu informatycznego) jednostkom organizacyjnym pomocy społecznej oraz jednostkom obsługującym świadczenia rodzinne danych osób, które nie ubiegają się o żadne świadczenia przyznawane przez te podmioty, stanowiło naruszenie art. 26 ust 1 pkt 1 ustawy o ochronie danych osobowych<sup>9</sup>, gdyż pozyskiwanie danych ww. osób przez te jednostki nie było niezbędne do realizacji zadań publicznych.

Ponadto Generalny Inspektor stwierdził, iż PUP nie zastosował odpowiednich środków technicznych (o których mowa w art. 36 ust. 1 ustawy)<sup>10</sup> w celu ochrony danych osobowych osób bezrobotnych i klientów PUP, gdyż nie zabezpieczył danych osobowych ww. osób przed ich udostępnieniem osobom nieupoważnionym i przetwarzaniem z naruszeniem ustawy. W związku ze stwierdzonymi w PUP uchybieniami w procesie przetwarzania danych osobowych, wobec PUP - jako administratora danych osobowych - zostało wszczęte postępowanie administracyjne w zakresie stwierdzonych uchybień.

## **2.2.2. Bezpieczeństwo publiczne**

W 2012 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził **11 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.

Tego typu kontrole zostały przeprowadzone w jednostkach Straży Granicznej (5 kontrole<sup>11</sup>), u wojewodów (3 kontrole<sup>12</sup>), w wydziałach konsularnych ambasad Rzeczypospolitej Polskiej (2 kontrole<sup>13</sup>) oraz w Centralnym Organie Technicznym KSI, którym jest Komendant Główny Policji. Zakresem kontroli objęto dane osobowe przetwarzane przez te podmioty w związku z realizacją ich uprawnień wynikających z przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. Nr 165, poz. 1170 z późn. zm.), tj. wglądu oraz dokonywania wpisów do SIS i VIS.

Kontrole przeprowadzone w jednostkach Straży Granicznej wykazały, że w zakresie objętym kontrolą nie dochodziło do naruszenia przepisów odnoszących się do przetwarzania danych osobowych

---

<sup>9</sup> 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.

<sup>10</sup> Art. 36 ust. 1. 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, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

<sup>11</sup> Np. kontrole DIS-K-421/98/12 i DIS-K-421/121/12.

<sup>12</sup> Np. kontrole DIS-K-421/118/12 i DIS-K-421/124/12.

<sup>13</sup> Kontrole DIS-K-421/157/12 i DIS-K-421/165/12.

w związku z dostępem do danych VIS. Zastosowane w tych jednostkach środki techniczne i organizacyjne w celu ochrony danych osobowych oraz podjęte działania kontrolne mające na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami, jednoznacznie potwierdziły dużą dbałość w tych jednostkach o bezpieczeństwo tych danych. Znacznie gorzej pod tym względem wypadły kontrole przeprowadzone u wojewodów. W jednej z tych kontroli stwierdzono przypadek nadania upoważnienia dla użytkownika indywidualnego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych osobie, która nie odbyła szkolenia z zakresu bezpieczeństwa i ochrony danych, co w konsekwencji oznaczało naruszenie art. 25 ust. 2 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym<sup>14</sup>. Inna kontrola przeprowadzona u wojewody wykazała natomiast, że nie były stosowane procedury kontrolne wskazujące działania podejmowane w celu zapewnienia zgodności wykorzystania danych z obowiązującymi przepisami oraz, że pracownikom upoważnionym do dostępu do danych VIS nie były wydawane zaświadczenia dotyczące odbycia szkolenia z zakresu bezpieczeństwa i ochrony danych.

Stosownie do art. 6 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym, również województwie posiadają bezpośredni dostęp do Wizowego Systemu Informacyjnego, realizowanego poprzez Krajowy System Informatyczny (KSI) umożliwiający wgląd do danych VIS w celu rozpatrywania wniosków wizowych. Wojewodowie mogą ponadto w systemie VIS rejestrować swoje decyzje o unieważnieniu, przedłużeniu lub cofnięciu wizy, jak również wykorzystywać ten system do sporządzania sprawozdań i statystyk, identyfikowania osoby, która nie spełnia lub przestała spełniać warunki wjazdu lub pobytu na terytorium państw członkowskich oraz innych obowiązków, o których mowa w art. 25 ust. 2 rozporządzenia w sprawie VIS.

Dostęp do danych VIS możliwy jest w urzędach wojewódzkich za pomocą aplikacji VIS WWW wykonanej przez Komendę Główną Policji. Nadzór nad tym kto, kiedy i w jakim zakresie miał dostęp do danych VIS za pośrednictwem wspomnianej aplikacji sprawuje Centralny Organ Techniczny KSI.

W toku kontroli przeprowadzonych u wojewodów ustalono, że aplikacja WWW VIS posiadała błędy uniemożliwiające wprowadzenie do Wizowego Systemu Informacyjnego informacji związanych z przedłużeniem ważności wizy Schengen. Po wpisaniu danych osoby ubiegającej się o przedłużenie ważności wizy Schengen, aplikacja ta generowała błąd, który nie pozwalał na wprowadzenie informacji dotyczących przedłużonej wizy Schengen do tego systemu. W celu wyjaśnienia przyczyn zaistnienia ww. błędu została przeprowadzona kontrola w Centralnym Organie Technicznym KSI.

---

<sup>14</sup> Art. 25. 1. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny (KSI) jest obowiązany do przeszkolenia z zakresu bezpieczeństwa i ochrony danych wszystkich osób mających dostęp do Krajowego Systemu Informatycznego (KSI). 2. Odbycie szkolenia, o którym mowa w ust. 1, jest warunkiem otrzymania upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych.

Wykazała ona, że powodem występowania błędu była niepoprawna długość identyfikatora wniosku o przedłużenie ważności wizy Schengen, który był nadawany automatycznie przez aplikację WWW VIS (identyfikator ten był za krótki). Z informacji uzyskanych w toku wskazanej kontroli wynikało, że błąd ten został już naprawiony przez informatyków zatrudnionych w Komendzie Głównej Policji.

Uchybienie w procesie przetwarzania danych osobowych stwierdzone zostało również podczas kontroli przeprowadzonej w jednym z wydziałów konsularnych ambasady Rzeczypospolitej Polskiej. Polegało ono na niewdrożeniu dokumentacji stanowiącej instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, w zakresie formy wniosku o nadanie uprawnień w systemie informatycznym wykorzystywanym m.in. do dostępu do danych SIS. Z ustaleń kontrolnych wynikało bowiem, że taki wniosek składany był ustnie przez kierownika wydziału konsularnego, podczas gdy zgodnie z ww. dokumentacją powinien on mieć formę pisemną. Zastrzeżenia wzbudził również fakt, że zadania administratora bezpieczeństwa informacji w placówkach zagranicznych wykonywał administrator bezpieczeństwa informacji wyznaczony w Ministerstwie Spraw Zagranicznych, co powodowało wątpliwości co do skuteczności realizacji przez tę osobę nadzoru nad przestrzeganiem zasad ochrony danych osobowych w tych placówkach.

W 2012 r. w związku z przetwarzaniem danych osobowych w Krajowym Systemie Informatycznym, zostały również dokonane czynności kontrolne w sądach okręgowych (3 kontrole<sup>15</sup>) oraz prokuraturach okręgowych (3 kontrole<sup>16</sup>). Ich zakresem objęto wpisy w Systemie Informacyjnym Schengen (SIS) dokonywane na podstawie art. 95 Konwencji Wykonawczej do Układu z Schengen z dnia 14 czerwca 1985 r. 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.)<sup>17</sup>, w związku z decyzją Wspólnego

---

<sup>15</sup> Np. kontrole DIS-K-421/16/12 i DIS-K-421/17/12.

<sup>16</sup> Np. kontrole DIS-K-421/26/12 i DIS-K-421/34/12.

<sup>17</sup> Art. 95. 1. Dane na temat osób poszukiwanych do aresztowania ekstradycyjnego są wprowadzane na wniosek władzy sądowej wzywającej Umawiającą się Stronę. 2. Do czasu wprowadzenia wpisu, Umawiająca się Strona sprawdzi, czy aresztowanie jest dozwolone na mocy prawa krajowego wezwanej Umawiającej się Strony. Jeśli Umawiająca się Strona wprowadzająca wpis ma jakiegokolwiek wątpliwości, powinna zasięgnąć opinii innych zainteresowanych Umawiających się Stron. Umawiająca się Strona wprowadzająca wpis przesyła wezwanym Umawiającym się Stronom najszybszymi sposobami zarówno wpis, jak i następujące podstawowe informacje odnoszące się do danej sprawy: a) organ, który wydał wniosek o aresztowanie; b) informację, czy istnieje nakaz aresztowania lub inny dokument mający identyczny skutek prawny, lub podlegający wykonaniu wyrok; c) charakter i kwalifikację prawną przestępstwa; d) opis okoliczności, w których przestępstwo zostało popełnione, w tym czas, miejsce oraz stopień udziału w przestępstwie osoby, w przypadku której wpis został wprowadzony; e) tak dalece jak to możliwe, konsekwencje popełnienia przestępstwa. 3. Wezwana Umawiająca się Strona może dodać do pliku danych w swoim krajowym module Systemu Informacyjnego Schengen zastrzeżenie zakazujące aresztowania na podstawie wpisu do czasu usunięcia zastrzeżenia. Zastrzeżenie powinno zostać usunięte nie później niż 24 godziny po wprowadzeniu wpisu, o ile Umawiająca się Strona odmawia dokonania żądanego aresztowania z uwagi na przyczyny prawne lub ze względów praktycznych. W szczególnych sytuacjach, kiedy jest to uzasadnione skomplikowanym charakterem faktów leżących u podstaw wpisu, wyżej wymieniony termin może być przedłużony do jednego tygodnia. Bez uszczerbku dla wprowadzonego zastrzeżenia lub decyzji w sprawie odmowy aresztowania pozostałe Umawiające się Strony mogą dokonać aresztowania żądanego we wpisie. 4. Jeśli ze szczególnie pilnych powodów Umawiająca się Strona zażąda przeprowadzenia natychmiastowej rewizji, wezwana Umawiająca się Strona zbada, czy jest w stanie wycofać wprowadzone zastrzeżenie. Wezwana Umawiająca się Strona podejmie niezbędne

Organu Nadzorczego Schengen (WON Schengen) o przeprowadzeniu audytu tych wpisów w sposób wskazany w kwestionariuszu przygotowanym przez WON Schengen. Przed przystąpieniem do czynności kontrolnych zostały wytypowane wpisy o numerach ID Schengen, które miały zostać poddane sprawdzeniu. Sądy i prokuratury objęte kontrolą przygotowały na tej podstawie akta dotyczące spraw, w których wydano Europejski Nakaz Aresztowania (ENA). W toku kontroli dokonano oględzin akt sądowych oraz prokuratorskich prowadzonych w związku z wydawaniem ENA. W organach, w których dokonano ponad 100 wpisów do SIS oględzinami zostało objętych 30 akt (2 kontrole), zaś tam, gdzie dokonano więcej niż 20 wpisów, ale mniej niż 100 – 20 akt (4 kontrole). Łącznie skontrolowano 140 akt sądowych, zawierających ENA. Za pośrednictwem aplikacji SISOne4All dokonano wglądu do danych SIS w zakresie wpisów oznaczonych ww. numerami ID Schengen. Dane zawarte we wpisach porównano z ENA, na podstawie których zostały dokonane. W taki sposób inspektorzy sprawdzili 140 wpisów.

W wyniku ww. kontroli ustalono, że zawartość wpisów była zgodna z art. 95 Konwencji. Dane były aktualne, przetwarzane zgodnie z prawem, przechowywane przez określony czas, a przekazywanie danych było zapisywane. Ponadto ustalono, że w większości przypadków dane były zgodne z prawdą. Tylko w niektórych, pojedynczych przypadkach porównanie zawartych w aktach sądowych danych dotyczących osób poszukiwanych z wpisami dokonanymi w SIS wykazało błędy. Na przykład w kilku wpisach do SIS nie było wpisane drugie imię poszukiwanego, mimo iż z ENA wynikało, że osoby te mają dwa imiona; w jednym przypadku zostały wpisane znaki szczególne, co nie wynikało z ENA, a w innym zaś nie wpisano znaków szczególnych, pomimo zawarcia takich informacji w ENA; w jednym wpisie brak było informacji o obywatelstwie poszukiwanego; w jednym wpisie zachodziła rozbieżność, co do daty urodzenia w zakresie oznaczenia dnia, a w innym wpisie – roku. Ustalono również, iż wpisy w SIS w zakresie imion, nazwisk i miejsc urodzenia były dokonywane bez użycia polskich znaków diakrytycznych.

W związku z dokonanymi w ww. zakresie ustaleniami, Generalny Inspektor skierował do Komendanta Głównego Policji, jako Centralnego Organu Technicznego KSI, pismo z prośbą o wyjaśnienie wskazanych błędów we wpisach do SIS<sup>18</sup>. Z udzielonych przez Centralny Organ Techniczny KSI wyjaśnień wynikało, że rozbieżności były wynikiem dopisania do wpisów w SIS określonych (uzupełniających) informacji przez operatora Biura SIRENE w oparciu o dokonaną weryfikację danych, np. w bazie PESEL. Wskazano również, że w związku z zaistniałą sytuacją

---

kroki w celu zapewnienia, aby działania zostały przeprowadzone niezwłocznie po potwierdzeniu wpisu. 5. Jeśli aresztowanie nie może być dokonane z uwagi na nie zakończenie dochodzenia lub dlatego że wezwana Umawiająca się Strona go odmawia, Strona ta powinna uznać wpis za wpis do celów podania miejsca pobytu danej osoby. 6. Wezwane Umawiające się Strony przeprowadzają działania wymagane we wpisie zgodnie z obowiązującymi konwencjami o ekstradycji oraz prawem krajowym. Nie są one zobowiązane do przeprowadzania żądanych działań, jeśli dotyczą one jednego z jej obywateli, bez uszczerbku dla możliwości aresztowania tej osoby zgodnie z prawem krajowym.

<sup>18</sup> Pisma z dnia 26 kwietnia 2012 r. i z dnia 13 czerwca 2012 r.

Dyrektor Biura Międzynarodowej Współpracy Policji, nadzorujący Biuro SIRENE, został poinformowany o braku podstaw prawnych do tego typu działań operatorów Biura SIRENE oraz o konieczności zwrócenia się w takim przypadku do właściciela wpisu z wnioskiem o jego modyfikację.

### **2.2.3. Banki i inne instytucje finansowe**

W 2012 r. przeprowadzono **16 kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w podmiotach sektora bankowego.**

Wśród skontrolowanych podmiotów znalazło się 9 banków spółdzielczych i 2 banki zrzeszających banki spółdzielcze<sup>19</sup>. Zakresem kontroli objęto udostępnianie przez banki spółdzielcze danych osobowych swoich klientów Biuru Informacji Kredytowej S.A. z siedzibą w Warszawie (dalej: BIK).

W toku kontroli ustalono, że każdy z banków zrzeszających zawarł z BIK umowę w sprawie gromadzenia, przetwarzania i udostępniania informacji, określającą zasady współpracy w zakresie gromadzenia, przetwarzania i udostępniania bankowi informacji stanowiących tajemnicę bankową na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.), w zakresie, w jakim informacje te były potrzebne w związku z wykonywaniem czynności bankowych oraz udostępniania przez BIK innych produktów i usług wspomagających ocenę zdolności kredytowej oraz analizę ryzyka kredytowego. Na podstawie ww. umów banki zrzeszające zobowiązały się przekazywać BIK dane klientów (swoich klientów, jak również klientów zrzeszonych banków spółdzielczych, które przystąpiły do umowy) w formie zapytań i wsadów informacyjnych. Natomiast BIK zobowiązał się udostępniać raporty oraz inne produkty i usługi wspomagające w wykonywaniu czynności bankowych, w tym zwłaszcza w podejmowaniu decyzji kredytowych.

Zgodnie z postanowieniami omawianych umów wsad informacyjny stanowią dane o klientach banku (banku zrzeszającego, banku spółdzielczego zrzeszonego), znajdujące się w bazach danych banku i zawierające, stosownie do art. 105 ust. 4 ustawy Prawo bankowe, informacje objęte tajemnicą bankową w zakresie, w jakim informacje te są potrzebne w związku z wykonywaniem czynności bankowych i przekazywane cyklicznie przez bank do BIK. Natomiast zbiorczy wsad informacyjny jest to odrębny plik, w którym scalone są wsady informacyjne pochodzące z poszczególnych banków, przy czym każdy zbiorczy wsad informacyjny powinien umożliwiać identyfikację wsadu informacyjnego poszczególnych banków. W przypadku powzięcia przez bank zrzeszający wiarygodnej informacji, że dane nadesłane do BIK z jakiegokolwiek powodu stały się nieaktualne, niekompletne, nieprawdziwe lub niedokładne, bank zrzeszający niezwłocznie dokonuje korekty ww. danych.

---

<sup>19</sup> Np. kontrole: DIS-K-421/21/12, DIS-K-421/28/12, DIS-K-421/37/12.

Na podstawie wyników kontroli zastrzeżenia wzbudziła stwierdzona liczba nieaktualizowanych przez banki spółdzielcze rachunków osób fizycznych (wyrażona w ujęciu procentowym w stosunku do ilości wszystkich czynnych rachunków kredytowych). Jak ustalono, znaczące obniżenie liczby nieaktualizowanych rachunków w ramach sektora banków spółdzielczych było możliwe do uzyskania, gdyż w części banków spółdzielczych (w których kontrole nie były przeprowadzone) stopień aktualizacji rachunków kształtował się na bardzo niskim poziomie i w ten sposób zawyżana była średnia nieaktualizowanych rachunków przekazywanych do BIK w ramach poszczególnych zrzeszeń. Należy wskazać, że przepisy Prawa bankowego po zaistnieniu określonych przesłanek zezwalają bankom na przekazywanie danych osobowych klientów do BIK, jak również dalsze ich przetwarzanie przez ten podmiot. Niemniej jednak brak aktualności danych może skutkować zaistnieniem sytuacji, w której przesłanki umożliwiające przetwarzanie danych nie będą zachodziły, a zatem proces ten będzie bezprawny. Stosownie do art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, obowiązek dochowania szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, polega między innymi na wymogu zapewnienia merytorycznej poprawności danych (zasada prawdziwości danych). W literaturze przedmiotu podkreśla się, że wynikające z tych danych informacje powinny być zgodne z prawdą, pełne (kompletne) oraz odpowiadać aktualnemu (najnowszemu) stanowi rzeczy<sup>20</sup>. W świetle powyższego obowiązkiem banków było zapewnienie prawdziwości, kompletności i aktualności danych poprzez poinformowanie BIK o zaistniałych zmianach bez zbędnej zwłoki. Obowiązek administratora danych do bezzwłocznego informowania innych administratorów danych, którym udostępnił zbiór danych, o dokonanych uaktualnieniach lub sprostowaniach przekazanych im danych, został również wyrażony w art. 35 ust. 3 ustawy o ochronie danych osobowych<sup>21</sup>.

W związku z powyższymi ustaleniami, Generalny Inspektor skierował do Przewodniczącego Komisji Nadzoru Finansowego pismo z prośbą o podjęcie działań zmierzających do zwrócenia uwagi bankom spółdzielczym i bankom zrzeszającym, na konieczność dostosowania procesu przetwarzania danych osobowych do wymogów ustawy o ochronie danych osobowych, polegających na obowiązku uaktualniania bez zbędnej zwłoki, danych osobowych ich klientów przekazywanych BIK<sup>22</sup>.

Na podstawie całokształtu materiału dowodowego zgromadzonego w toku czynności kontrolnych przeprowadzonych w bankach spółdzielczych i w bankach zrzeszających, nie stwierdzono natomiast uchybień w zakresie zabezpieczenia danych osobowych przetwarzanych zarówno w systemach informatycznych, jak i w postaci tradycyjnej. Banki zastosowały w procesie udostępniania danych do BIK środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do

---

<sup>20</sup> J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*. Wolters Kluwer Polska Sp. z o.o., Warszawa 2007, s. 507.

<sup>21</sup> Art. 35. 3. Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanych uaktualnieniach lub sprostowaniach danych.

<sup>22</sup> Pismo z dnia 17 lipca 2012 r. sygn. DIS-424/44035/12.

zagrożeń oraz kategorii danych objętych ochroną. W szczególności dane zostały zabezpieczone przed ich udostępnieniem osobom nieupoważnionym.

W okresie sprawozdawczym, w związku z pismami Generalnego Inspektora Informacji Finansowej (dalej: GIIF) informującymi o nieprawidłowościach w zakresie przestrzegania przepisów o ochronie danych osobowych przez instytucje obowiązane, tj. podmioty wskazane w art. 2 ust. 1 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.), zwaną dalej ustawą o PPP, w ramach realizacji zadań związanych z prowadzeniem rejestru transakcji, o którym mowa w art. 8 ust. 1 ustawy o PPP<sup>23</sup>, zostały przeprowadzone czynności kontrolne w trzech instytucjach obowiązanych, tj. banku, towarzystwie ubezpieczeniowym oraz towarzystwie funduszy inwestycyjnych. GIIF wskazał bowiem, iż w rejestrze transakcji rejestrowane były także transakcje, które nie podlegały obowiązkowi rejestracji, co skutkuje przetwarzaniem przez instytucje obowiązane danych osobowych bez podstawy prawnej i może stanowić naruszenie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych<sup>24</sup>.

Należy wskazać, iż powołany rejestr prowadzony był na podstawie rozporządzenia Ministra Finansów z dnia z dnia 21 września 2001 r. w sprawie określenia wzoru rejestru transakcji, sposobu jego prowadzenia oraz trybu dostarczania danych z rejestru Generalnemu Inspektorowi Informacji Finansowej (Dz. U. Nr 113, poz. 1210 z późn. zm.). W podmiotach kontrolowanych, na podstawie art. 10a ust. 1 ustawy o PPP<sup>25</sup>, zostały wprowadzone w formie pisemnej wewnętrzne procedury w sprawie przeciwdziałania praniu pieniędzy i zwalczania terroryzmu. Procedury te określają m.in. sposób prowadzenia rejestru transakcji, przekazywania i archiwizowania danych w nim zawartych oraz zasady przekazywania informacji do GIIF o zarejestrowanych transakcjach. W rejestrze tym znajdowały się informacje dotyczące transakcji, których równowartość przekraczała 15 tys. EURO - zarówno w odniesieniu do transakcji prowadzonej w ramach jednej operacji, jak też w ramach kilku operacji, jeżeli okoliczności wskazują, że są one ze sobą powiązane i zostały podzielone na operacje o mniejszej wartości z zamiarem uniknięcia obowiązku rejestracji.

Podstawą prawną legitymującą instytucje obowiązane do przetwarzania danych osobowych w rejestrze transakcji są przepisy ustawy o PPP (m.in. art. 9 ust. 1<sup>26</sup>) oraz rozporządzenia w sprawie

---

<sup>23</sup> Art. 8. 1. Instytucja obowiązana przeprowadzająca transakcję, której równowartość przekracza 15.000 euro, ma obowiązek zarejestrować taką transakcję również w przypadku, gdy jest ona przeprowadzana za pomocą więcej niż jednej operacji, których okoliczności wskazują, że są one ze sobą powiązane i zostały podzielone na operacje o mniejszej wartości z zamiarem uniknięcia obowiązku rejestracji.

<sup>24</sup> Art. 23.1.2. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

<sup>25</sup> Art. 10a. 1. Instytucje obowiązane wprowadzają w formie pisemnej wewnętrzną procedurę w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

<sup>26</sup> Art. 9.1.1. Identyfikacja, o której mowa w art. 8b ust. 3 pkt 1, obejmuje: w przypadku osób fizycznych i ich przedstawicieli - ustalenie i zapisanie cech dokumentu stwierdzającego na podstawie odrębnych przepisów tożsamość osoby, a także imienia, nazwiska, obywatelstwa oraz adresu osoby dokonującej transakcji, a ponadto numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL, lub numeru dokumentu stwierdzającego tożsamość cudzoziemca, lub kodu kraju w przypadku przedstawienia paszportu.



określenia wzoru rejestru transakcji, sposobu jego prowadzenia oraz trybu dostarczania danych z rejestru Generalnemu Inspektorowi Informacji Finansowej.

Jak ustalono w toku przedmiotowych kontroli, dane przetwarzane w rejestrze transakcji pochodziły z systemów transakcyjnych instytucji obowiązanych (zbioru danych klientów), w których były przetwarzane na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.), ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.), ustawy z dnia 27 maja 2007 r. o funduszach inwestycyjnych (Dz. U. Nr 146, poz. 1546 z późn. zm.) oraz w celu realizacji umów zawartych z klientami. Zakres danych osobowych przetwarzanych w rejestrze wynika z przepisów ustawy o PPP oraz rozporządzenia w sprawie określenia wzoru rejestru transakcji, sposobu jego prowadzenia oraz trybu dostarczania danych z rejestru Generalnemu Inspektorowi Informacji Finansowej. Dane w rejestrze transakcji przetwarzane są w celu ich przekazania do GIIF oraz w celu realizacji przez instytucje obowiązywane innych obowiązków związanych z przeciwdziałaniem praniu pieniędzy, w tym bieżącego monitorowania stosunków gospodarczych (art. 8b ust. 3 ustawy o PPP).

Administrator zbioru danych osobowych przetwarzanych w rejestrze transakcji, o którym mowa w art. 8 ust. 1 ustawy PPP, jest zwolniony na podstawie art. 43 ust. 1 pkt 2a ustawy<sup>27</sup> z obowiązku zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

W świetle powyższych ustaleń brak było podstaw do uznania, że w ramach realizacji zadań związanych z prowadzeniem rejestru transakcji instytucje obowiązywane przetwarzają w zbiorze dane osobowe z naruszeniem art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

#### **2.2.4. Telekomunikacja**

W 2012 r. przeprowadzono **5 kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych u operatorów publicznej sieci telekomunikacyjnej, dostawców publicznie dostępnych usług telekomunikacyjnych**<sup>28</sup>. Zakresem kontroli objęto realizację przez przedsiębiorców telekomunikacyjnych obowiązków, o których mowa w art. 180a, 180b, 180c, 180d, 180e ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)<sup>29</sup> oraz prawidłowość gromadzenia i przekazywania danych telekomunikacyjnych zgodnie z trybem i warunkami przewidzianymi w rozporządzeniu Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do

---

<sup>27</sup> Art. 43.1.2a Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych przez Generalnego Inspektora Informacji Finansowej.

<sup>28</sup> Np. kontrole: DIS-K-421/117/12, DIS-K-421/125/12 i DIS-K-421/126/12.

<sup>29</sup> Art. 180b. 1. Obowiązek, o którym mowa w art. 180a ust. 1, może być wykonywany wspólnie przez dwóch lub więcej operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych. 2. Operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych może powierzyć realizację obowiązku, o którym mowa w art. 180a ust. 1, w drodze umowy, innemu przedsiębiorcy telekomunikacyjnemu. Powierzenie to nie zwalnia powierzającego z odpowiedzialności za realizację tego obowiązku.

przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023).

W toku przeprowadzonych kontroli ustalono, iż objęci kontrolami przedsiębiorcy telekomunikacyjni realizowali obowiązek zatrzymania i przechowywania danych, o których mowa w art. 180c Prawa telekomunikacyjnego, tj. danych niezbędnych do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz tego do którego kierowane jest połączenie, a także określenia daty i godziny połączenia oraz czasu jego trwania, określenia rodzaju połączenia i lokalizacji telekomunikacyjnego urządzenia końcowego. Zakres zatrzymywanych i przechowywanych danych określa 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 zatrzymania i przechowywania (Dz. U. Nr 226, poz. 1828). Zakres ten 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 i usługi połączeń telefonicznych w technologii VOIP. Dane, o których mowa w art. 180c Prawa telekomunikacyjnego, dla których upłynął okres 24 miesięcy licząc od dnia połączenia lub nieudanej próby połączenia, były usuwane z systemów informatycznych: automatycznie poprzez wdrożenie niezbędnych mechanizmów w tych systemach (zdefiniowanie procedur dotyczących usuwania danych) lub ręcznie przez administratora systemu (innego upoważnionego pracownika).

Niektóre skontrolowane podmioty realizowały samodzielnie obowiązek, o którym mowa w art. 180a ust. 1 pkt 1 Prawa telekomunikacyjnego, część powierzyła w całości lub w części realizację tego obowiązku innym podmiotom na podstawie zawartych w tym zakresie umów, zgodnie z art. 180b ust. 2 Prawa telekomunikacyjnego (np. w zakresie usługi poczty elektronicznej, telefonii stacjonarnej).

W celu ochrony danych, o której mowa w art. 180a ust. 1 pkt 3 Prawa telekomunikacyjnego, przedsiębiorcy telekomunikacyjni stosowali właściwe środki techniczne i organizacyjne oraz zapewniali dostęp do tych danych jedynie upoważnionym pracownikom, zgodnie z przepisami art. 180e ustawy Prawo telekomunikacyjne. Dostęp do danych retencyjnych posiadali wyłącznie upoważnieni pracownicy, których upoważnienia do przetwarzania danych osobowych ujęte były w ewidencjach osób zatrudnionych przy przetwarzaniu danych osobowych. Przedsiębiorcy telekomunikacyjni prowadzili dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. W kontrolowanych podmiotach wyznaczeni zostali administratorzy bezpieczeństwa informacji oraz

sprawowana była kontrola nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane.

Ponadto wskazać należy, iż nowelizacja Prawa telekomunikacyjnego, która weszła w życie w dniu 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. UrzUE z 2006 r. Nr 105 poz. 54). Zgodnie z art. 7 dyrektywy 2006/24/WE, 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.

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 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. Zatem uznano, że obowiązek usuwania danych po upływie 24 miesięcy nie jest obowiązkiem bezwzględnym. W prawie polskim dłuższe przechowywanie jest możliwe, jeżeli dane zostały „zabezpieczone, zgodnie z przepisami odrębnymi”. Natomiast dyrektywa 2006/24/WE z obowiązku zniszczenia zwalnia te dane, które zostały udostępnione i zachowane. Jak ustalono w toku jednej z kontroli, skany zapytań przechowywane były w systemie informatycznym przez około 2 lata, a pytania zadane w formie elektronicznej oraz udzielone odpowiedzi przez okres około 6 miesięcy. Po upływie ww. terminów omawiane dokumenty archiwizowane były w systemie informatycznym (archiwum). W związku z powyższym uznano, że użyty w art. 180a ust. 1 pkt 1 Prawa telekomunikacyjnego termin „zabezpieczone zgodnie z przepisami odrębnymi” nie był

wystarczająco precyzyjnie określony, zatem należy interpretować go zgodnie z postanowieniami ww. dyrektywy, tj. uznać, że dane, które już zostały udostępnione, mogą być przechowywane dłużej, np. w celach archiwalnych, zgodnie z obowiązującymi u operatorów procedurami.

W toku przeprowadzonych kontroli nie stwierdzono uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą. Zwrócono natomiast uwagę na pewne odmienności w interpretacji przepisów dotyczących badanych zagadnień. Podniesione na skutek przedmiotowych kontroli uwagi wynikające z braku jednoznaczności w przepisach Prawa telekomunikacyjnego, nie stanowiły naruszenia przepisów o ochronie danych osobowych. Zatem brak było podstaw do zastosowania przez Generalnego Inspektora uprawnień, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych<sup>30</sup>.

### 2.2.5. Zatrudnienie

W toku kontroli przeprowadzonej w jednej ze spółek prowadzącej na podstawie koncesji Ministra Spraw Wewnętrznych i Administracji działalność gospodarczą w zakresie usług ochrony osób i mienia realizowanych w formie bezpośredniej ochrony fizycznej oraz zabezpieczenia technicznego ustalono, że w spółce tej prowadzone były wobec konwojentów i dyspozytorów badania poligraficzne. Badania te przeprowadzone zostały za pisemną zgodą pracowników. W związku z ww. badaniami pozyskiwano m.in. dane osobowe o stanie zdrowia oraz dane w zakresie wynikającym z odpowiedzi na poszczególne pytania odnoszące się do zachowań mających miejsce przed i podczas zatrudnienia w spółce. Generalny Inspektor stwierdził, że ustawową podstawę do żądania od osoby ubiegającej się o pracę oraz od pracownika ujawnienia danych osobowych związanych z zatrudnieniem stanowi art. 22<sup>1</sup> ustawy z dnia 26 czerwca 1996 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.)<sup>31</sup>. Wskazana spółka nie jest podmiotem uprawnionym na podstawie przepisów prawa pracy, ani innych przepisów regulujących wykonywaną przez nią działalność, w szczególności ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2005 r. Nr 145, poz. 1221 z późn. zm.), do pozyskiwania ww. danych dotyczących wskazanych kategorii pracowników. Generalny Inspektor uznał, że ustawodawca przyznając pracodawcy prawo do żądania od osoby ubiegającej się o pracę, a także od

---

<sup>30</sup> 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.

<sup>31</sup> Art. 22<sup>1</sup> Kodeksu pracy zezwala na gromadzenie przez pracodawcę trzech grup danych, tj. 1) danych osobowych wyliczonych w nim enumeratywnie – imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia (§ 1), 2) danych osobowych pracownika i jego dzieci, koniecznych ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, numeru PESEL pracownika (§ 2), 3) innych danych osobowych, jeżeli obowiązek ich podania wynika z odrębnych przepisów (§ 4).

pracownika, jedynie danych wskazanych w art. 22<sup>1</sup> Kodeksu pracy, zezwolił tym samym na przetwarzanie danych wyłącznie w tym zakresie i wyłączył możliwość żądania innych danych, to jest np. w oparciu o zgodę osoby, której dane dotyczą. Złożenie zatem przez pracownika oświadczenia, którego treścią jest wyrażenie zgody na przeprowadzenie badania wariograficznego, a tym samym na przetwarzanie jego danych osobowych, nie stanowi przesłanki legalizującej przetwarzanie danych osobowych tego pracownika pozyskanych w związku z badaniem. Przyjęcie odmiennej interpretacji skutkowałoby możliwością pozyskiwania danych osobowych od pracowników wbrew wyrażonym w powołanym przepisie intencjom ustawodawcy. Konsekwencją uznania zgody za przesłankę pozwalającą na zbieranie danych pracowników musiałaby być konieczność dokonania oceny, czy została ona wyrażona w sposób dobrowolny. Jak podkreśla się w literaturze, brak równowagi między pozycją pracodawcy a pracownika niweczy tę swobodę. „Wydaje się, że dopuszczenie przetwarzania danych na podstawie zgody w sytuacji, gdy przepisy ograniczają zakres przetwarzania danych, pozbawia sensu wspomniane ograniczenie, w szczególności wówczas, gdy osoba, której dane dotyczą, pozostaje w układzie podległości względem podmiotu, któremu zgoda ma być udzielona”<sup>32</sup>. W relacji zachodzącej między pracownikiem i pracodawcą występują okoliczności wpływające na brak omawianej równowagi, które sprzyjają wymuszaniu zgody, a tym samym pozbawiają ją przymiotu dobrowolności. Powoływanie jako przesłanki legalizującej przetwarzanie danych zgody pracownika, w sytuacji gdy przepisy wskazują katalog danych, które mogą być przez pracodawcę przetwarzane, prowadzi także do obchodzenia prawa regulującego te kwestie w sposób jednoznaczny. Skutkuje to poszukiwaniem innych podstaw do przetwarzania danych, niż te, które ustawodawca uznał za jedynie dopuszczalne. Generalny Inspektor odnosząc się do Opinii 8/2001 Grupy Roboczej Art. 29 z dnia 13 września 2001 r. w sprawie przetwarzania danych osobowych w kontekście zatrudnienia (WP48)<sup>33</sup> i wyroku Naczelnego Sądu Administracyjnego w Warszawie z dnia 13 lutego 2003 r. (II SA 1620/01)<sup>34</sup>, wskazał, że w związku z brakiem równorzędności stron w relacji pracodawca – pracownik, zgoda na przeprowadzenie badania poligraficznego nie może być uznana za oświadczenie woli wyrażone w sposób swobodny. W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych, wobec spółki jako administratora danych osobowych, zostało wszczęte postępowanie administracyjne. W odpowiedzi na pismo wszczynające postępowanie administracyjne

---

<sup>32</sup> Paweł Fajgielski, Zgoda na przetwarzanie danych. [w:] Grzegorz Sibiga, Xawery Konarski (red.), Ochrona danych osobowych. Aktualne problemy i nowe wyzwania, Oficyna a Wolters Kluwer business, Warszawa 2007, s. 47.

<sup>33</sup> W Opinii 8/2001 Grupy Roboczej Art. 29 z dnia 13 września 2001 r. w sprawie przetwarzania danych osobowych w kontekście zatrudnienia (WP48) stwierdza się, że „jeżeli pracodawca musi przetwarzać dane osobowe, co jest nieuniknioną i konieczną konsekwencją stosunku pracy, popełnia błąd jeżeli próbuje zalegalizować to przetwarzanie za pomocą zgody. Można posłużyć się zgodą, jeżeli odnosi się ona ściśle do przypadku, w którym pracownik ma całkowitą swobodę jej udzielenia i może odmówić jej udzielenia bez poniesienia szkody”.

<sup>34</sup> NSA w Warszawie w wyroku z dnia 13 lutego 2003 r. (II są 1620/01) stwierdził, że „skutki badań poligraficznych mimo że dobrowolnych, naruszają prawa i wolności badanych. Jak się zresztą wskazuje w literaturze, wyrażenie zgody na badania przy pomocy wykrywacza kłamstw, prowadzone przez pracodawcę, stawia pod znakiem zapytania swobodę tej zgody”.

spółka poinformowała, że zaprzestała prowadzenia badań poligraficznych pracowników i usunęła wszystkie dane osobowe pozyskane w związku z tymi badaniami.

W wyniku innej kontroli przeprowadzonej w jednej ze spółek stwierdzono, że podczas rozmów kwalifikacyjnych kandydaci do pracy otrzymywali do wypełnienia formularz aplikacyjny, za pomocą którego spółka pozyskiwała, m.in. informacje na temat mocnych i słabych stron kandydata. W oparciu o analizę obowiązujących przepisów<sup>35</sup> Generalny Inspektor Ochrony Danych Osobowych podniósł, że praktyka ta odbywała się z naruszeniem przepisów prawa.

W toku kontroli ustalono ponadto, że każda osoba zatrudniana na podstawie umowy o pracę wypełniała kwestionariusz osobowy, za pomocą którego spółka pozyskiwała informacje na temat stanu cywilnego nowo zatrudnianego (panna/kawaler, mężatka/żonaty, rozwiedziona/y, wdowa/wdowiec). Działanie takie również uznane zostało za sprzeczne z obowiązującym prawem<sup>36</sup>.

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych, wobec spółki zostało wszczęte postępowanie administracyjne. W toku postępowania spółka usunęła uchybienia stanowiące przedmiot postępowania. Z powyższych względów postępowanie zostało umorzone.

## 2.2.6. Służba zdrowia

W ramach tego sektora w 2012 r. skontrolowano **9 podmiotów**<sup>37</sup>, w tym siedem ośrodków dawców szpiku posiadających pozwolenie Ministra Zdrowia na wykonywanie czynności polegających na pozyskiwaniu potencjalnych dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej, w rozumieniu art. 16a ust. 1 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. Czynności kontrolne przeprowadzono również w Centrum Organizacyjno – Koordynacyjnym do spraw Transplantacji „Poltransplant”<sup>38</sup>, zwanym dalej Poltransplantem. Zakresem przeprowadzonych kontroli objęto dane osobowe potencjalnych dawców oraz dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej, przetwarzane przez skontrolowane podmioty jako ośrodki dawców szpiku.

---

<sup>35</sup> Art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych. Administrator 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. Art. 22<sup>1</sup> § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.). Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko, imiona rodziców, datę urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia. Art. 22<sup>1</sup> § 4 Kodeksu pracy. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

<sup>36</sup> Art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych. Administrator 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. Zob. także cytowane wcześniej przepisy Art. 22<sup>1</sup> § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.).

<sup>37</sup> Np. kontrole: DIS-K-421/75/12, DIS-K-421/76/12, DIS-K-421/81/12, DIS-K-421/92/12, DIS-K-421/109/12.

<sup>38</sup> DIS-K-421/135/12

Kontrole wykazały m.in., że na podstawie art. 16 ust. 5 ustawy transplantacyjnej, dane osobowe potencjalnych dawców allogenicznego szpiku komórek krwiotwórczych krwi obwodowej były udostępniane przez ośrodki dawców szpiku do „Centralnego rejestru niespokrewnionych potencjalnych dawców szpiku i krwi pępowinowej” (zwanego dalej Centralnym Rejestrem) prowadzonego przez Poltransplant. Powołany artykuł nakłada na ośrodki dawców szpiku obowiązek niezwłocznego przekazywania do ww. rejestru, danych osobowych potencjalnego dawcy w zakresie: imię i nazwisko, data i miejsce urodzenia, adres miejsca zamieszkania, numer PESEL, informacje o antygenach zgodności tkankowej, wskazanie podmiotu, który dokonał badania antygenów zgodności tkankowej oraz inne informacje medyczne o istotnym znaczeniu. Aktualnie przekazywanie ww. danych odbywało się poprzez system informatyczny Poltransplantu. W toku kontroli ustalono, że jeden z ośrodków dawców szpiku do chwili obecnej nie przekazał do Poltransplantu wszystkich pozyskanych danych osobowych potencjalnych dawców w celu włączenia ich do Centralnego Rejestru. Zatem w tym przypadku wskazany w art. 16 ust. 5 ustawy transplantacyjnej obowiązek nie był wypełniany. Natomiast zarejestrowane przez ww. ośrodek dawców szpiku dane potencjalnych dawców w zakresie numeru dawcy, jego wieku, płci i oznaczenia HLA były przezeń przekazywane do niemieckiego centralnego rejestru dawców szpiku na podstawie zgody udzielonej przez osoby, których dane dotyczyły.

Ustalono też, że ośrodki dawców szpiku pozyskiwały na piśmie od potencjalnych dawców oraz dawców, zgodę na przetwarzanie dotyczących ich danych osobowych. Tymczasem pozyskiwanie tych zgód było zbędne, skoro obowiązujące przepisy prawa uprawniały administratora do przetwarzania tych danych. Dla ośrodków dawców szpiku takimi przepisami są w szczególności przepisy 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.). Pozyskiwanie przez administratora danych zgody na przetwarzanie danych osobowych jako dodatkowej podstawy prawnej w sytuacji, gdy do ich przetwarzania uprawnia go przepis prawa, budzi uzasadnione wątpliwości, gdyż może wprowadzać w błąd osoby, których dane dotyczą, co do możliwości jej skutecznego wycofania. Problematykę ograniczeń w wykorzystywaniu zgody jako podstawy prawnej pozyskiwania danych osobowych podejmowała kilkakrotnie w swoich opiniach Grupa Robocza Art. 29 (m.in. w opinii w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji medycznej oraz w opinii w sprawie definicji zgody). Zgodnie z wyrażonym w nich stanowiskiem *„Zależność od uzyskania zgody powinna być ograniczona do przypadków, w których osoba, której dotyczą dane, może dokonać rzeczywistego, wolnego wyboru, przez co rozumie się również możliwość cofnięcia zgody bez żadnego uszczerbku”*, zatem *„Jeżeli, po wycofaniu zgody przetwarzanie danych osobowych jest kontynuowane na innej podstawie prawnej, mogą zostać podniesione wątpliwości co do oryginalnego wykorzystania zgody jako wstępnej podstawy prawnej: jeżeli przetwarzanie mogło mieć miejsce od*

*początku przy użyciu innej podstawy, stawianie osoby fizycznej w sytuacji, w której jest proszona o zgodę na przetwarzanie mogłoby być uznane za wprowadzające w błąd lub nierzetelne*". Pozyskiwanie przez ośrodki dawców szpiku zgody na przetwarzanie danych osobowych od potencjalnych dawców szpiku lub komórek macierzystych krwi, było zatem uzasadnione jedynie w odniesieniu do danych osobowych, do których gromadzenia nieuprawnniają ich przepisy prawa (np. będą to numery telefonów do kontaktu z potencjalnym dawcą oraz jego adres e-mail). Natomiast w zakresie danych wskazanych w art. 16a ust. 8 ustawy transplantacyjnej, ośrodki dawców szpiku powinny zaprzestać jej pozyskiwania.

Zgodnie z art. 4 ust. 3 pkt 1 i 2 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. z 1997 r. Nr 106, poz. 681 z późn. zm.), jednostkami organizacyjnymi publicznej służby krwi są: instytut naukowo-badawczy, którego zadania określa art. 25, zwany dalej „instytutem” oraz regionalne centra krwiodawstwa i krwiolecznictwa, zwane dalej „regionalnymi centrami”. Jak wynika z art. 25 pkt 12 ww. ustawy, do zadań instytutu w zakresie publicznej służby krwi należy w szczególności określanie medycznych zasad pobierania krwi, oddzielania jej składników i wydawania, obowiązujących w jednostkach organizacyjnych publicznej służby krwi. Jak ustalono, poddany kontroli Instytut Hematologii i Transfuzjologii w Warszawie opracował „Medyczne zasady pobierania krwi, oddzielania jej składników i wydawania, obowiązujące w jednostkach organizacyjnych publicznej służby krwi”. Publikacja ta zawiera m.in. ogólne zasady rekrutacji przez jednostki publicznej służby krwi (ośrodki dawców szpiku) niespokrewnionych dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej (krwiotwórczych komórek macierzystych – dalej KKM). W rozdziale 12.3.1 wspomnianego opracowania wskazano m.in. że: *„Kandydat na dawcę KKM musi wypełnić indywidualną wstępną ankietę zdrowotną dawcy KKM, której przykład zamieszczono w p. 12.3.4. oraz podpisać deklarację przystąpienia do rejestru niespokrewnionych dawców szpiku, której przykłady znajdują się w punktach 12.3.5. i 12.3.6.”*. Powołany punkt 12.3.6. zawierał formularz Karty Ewidencyjnej Ogólnopolskiego Centralnego Rejestru Dawców Szpiku i Krwi Pępowinowej, który - jak ustalono - został opracowany przez Poltransplant, i który wykorzystywany był przez część skontrolowanych ośrodków dawców szpiku, w szczególności ośrodki będące jednostkami publicznej służby krwi. Te ostatnie realizują bowiem swoje zadania w oparciu o wytyczne zawarte w opisanych powyżej „Medycznych zasadach pobierania krwi, oddzielania jej składników i wydawania, obowiązujących w jednostkach organizacyjnych publicznej służby krwi”, dotyczące zasad rekrutacji i typowania tkankowego rodzinnych i niespokrewnionych dawców krwiotwórczych komórek macierzystych. Powyższy formularz zawierał w swej treści klauzulę zgody na przetwarzanie danych osobowych, pomimo iż dla części pozyskiwanych na jego podstawie danych (takich jak: imię, nazwisko, data i miejsce urodzenia, numer PESEL, adres zamieszkania) podstawę prawną przetwarzania stanowił art. 16a ust. 8 pkt 1 – 4 ustawy transplantacyjnej. Kwestia nieuzasadnionego



pozyskiwania zgody na przetwarzanie danych osobowych w sytuacji, gdy do ich przetwarzania uprawniana administratora danych przepisy prawa, została opisana powyżej. Podkreślenia wymaga natomiast, że w odniesieniu do danych osobowych wykraczających poza zakres wskazany w art. 16 ust. 8 ustawy transplantacyjnej ustalono, iż w formularzu tym nie zapewniono potencjalnym dawcom możliwości wyboru w zakresie wyrażenia/niewyrażenia zgody na ich przetwarzanie. Udzielenie ww. zgody następuje bowiem poprzez złożenie podpisu pod wszystkimi zawartymi w tym formularzu oświadczeniami. Należy bowiem podkreślić, iż klauzula o treści: „*Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z Ustawą z dnia 29.08.1997 o Ochronie Danych Osobowych (Dziennik Ustaw nr 133 poz 883)*”, jest tylko jednym z oświadczeń zawartych w opisywanym formularzu. Jednocześnie trzeba zauważyć, że z klauzuli tej nie wynika, które z danych pozyskiwanych na podstawie wymienionego powyżej formularza będą przetwarzane na podstawie zgody potencjalnego dawcy. W formularzu bowiem nie zaznaczono tych danych żadnym znacznikiem.

Kolejną kwestią wymagającą poruszenia było pozyskiwanie przez ośrodki dawców szpiku na podstawie formularza o nazwie „Karta Ewidencyjna Ogólnopolskiego Centralnego Rejestru Dawców Szpiku i Krwi Pępowinowej”, danych o nazwisku panieńskim potencjalnych dawców płci żeńskiej. Jak ustalono dane te przetwarzane były w celu identyfikacji ww. osób. Biorąc jednak pod uwagę, że dla tego samego celu ośrodki dawców szpiku pozyskują także takie dane, jak imię i nazwisko, data i miejsce urodzenia, a w szczególności numer PESEL umożliwiający jednoznaczne zidentyfikowanie osoby, której został on przypisany, uznać należy, że pozyskiwanie dodatkowo od potencjalnej dawczyni nazwiska panieńskiego było zbieraniem danych „na zapas”. W konsekwencji można zatem stwierdzić, że gromadzenie tych danych było nieadekwatne do celu ich przetwarzania, gdyż ten mógł być osiągnięty na podstawie węższego katalogu danych.

Potwierdziły to wyniki kontroli przeprowadzonej w Poltransplancie, który opracował ww. formularz. W toku czynności kontrolnych ustalono bowiem, że nazwisko panieńskie było informacją zbędną dla realizacji celu, jakim jest jak najszybszy dobór dawcy dla zgodnego pacjenta wymagającego leczenia przeszczepem szpiku i nie powinno być pozyskiwane od potencjalnych dawców przez ośrodki dawców szpiku. Ustalono też, że Poltransplant nie opracowywał ww. formularza dla obecnie działających ośrodków dawców szpiku. Formularz ten był zamieszczony na stronie internetowej Poltransplantu i stosowany w okresie, gdy podmiot ten sam rekrutował potencjalnych dawców<sup>39</sup> na analogicznych zasadach, jak obecnie działające ośrodki dawców szpiku. Jeżeli ośrodki dawców szpiku korzystały z jego wzoru, to prawdopodobnie stosowały ten formularz zastępczo, informując tym samym, że administratorem danych osobowych potencjalnych dawców jest również Poltransplant,

---

<sup>39</sup> Wskazywała na to nazwa ww. formularza, która mówił o Ogólnopolskim Centralnym Rejestrze Dawców Szpiku i Krwi Pępowinowej, prowadzonym przez Poltransplant od 2001 r. do 1 stycznia 2006 r., tj. do dnia wejścia w życie ustawy transplantacyjnej.

który na mocy przepisów ww. ustawy prowadzi Centralny Rejestr Niespokrewnionych Potencjalnych Dawców Szpiku i Krwi Pępowinowej. Również procedury opracowywane przez Instytut Hematologii i Transfuzjologii w Warszawie dla regionalnych centrów krwiodawstwa w zakresie ich działalności, jako jednostek publicznej służby krwi, nie były przedstawiane ani konsultowane z Poltransplantem.

Mając powyższe na uwadze stwierdzono, iż formularz Karty Ewidencyjnej Ogólnopolskiego Centralnego Rejestru Dawców Szpiku i Krwi Pępowinowej powinien zostać zmodyfikowany w taki sposób, aby osoby, których dane były pozyskiwane na ww. formularzu, nie były wprowadzane w błąd co do zbiorów danych, w których są one przetwarzane, podstaw prawnych przetwarzania tych danych oraz aby w odniesieniu do danych podawanych opcjonalnie (wykraczających poza zakres wskazany w art. 16a ust. 8 ustawy transplantacyjnej) zapewniona została swoboda wyrażenia przez potencjalnego dawcę zgody na przetwarzanie jego danych osobowych, oraz by dane te były adekwatne do celów ich przetwarzania.

Zastosowanie w zakresie ww. nieprawidłowości uprawnień przysługujących Generalnemu Inspektorowi na podstawie art. 18 ust. 1 pkt 1 ustawy o ochronie danych osobowych, wyłącznie wobec ośrodków dawców szpiku nienależących do jednostek publicznej służby krwi (których nie obowiązują zasady opracowywane przez Instytut Hematologii i Transfuzjologii) uznano jednak za niecelowe, gdyż prowadziłoby to do różnego traktowania w tym samym stanie faktycznym tej samej kategorii podmiotów. Dlatego w opisywanym przypadku do Instytutu Hematologii i Transfuzjologii z siedzibą w Warszawie, skierowane zostało wystąpienie o dostosowanie regulacji zawartych w „Medycznych zasad pobierania krwi, oddzielania jej składników i wydawania, obowiązujących w jednostkach organizacyjnych publicznej służby krwi” do przepisów o ochronie danych osobowych poprzez niezbędną modyfikację formularza Karty Ewidencyjnej Ogólnopolskiego Centralnego Rejestru Dawców Szpiku i Krwi Pępowinowej. Niezależnie od powyższego informacja o konieczności dostosowania ww. formularza do przepisów o ochronie danych osobowych została przesłana do ośrodków dawców szpiku wykorzystujących ten formularz.

Ponadto w toku trzech kontroli, które odbyły się w ośrodkach dawców szpiku ustalono, że ośrodki te uzyskały część przetwarzanych danych osobowych potencjalnych dawców od Poltransplantu. Dane tych potencjalnych dawców pozyskane zostały przez inne podmioty, które następnie albo nie otrzymały zezwolenia Ministra Zdrowia na wykonywanie czynności polegających na pozyskiwaniu potencjalnych dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej, albo nie utworzyły ośrodków dawców szpiku po wejściu w życie ustawy transplantacyjnej. Decyzję o przyznaniu kontrolowanym ośrodkom dawców szpiku dostępu do danych tych osób podejmował za każdym razem Poltransplant. Jednocześnie ustalono, iż tylko jeden z tych ośrodków realizował wobec osób, których ww. dane dotyczyły, obowiązek informacyjny wskazany

w art. 25 ust. 1 ustawy o ochronie danych osobowych<sup>40</sup>, każdorazowo podczas kontaktowania się z nimi.

W związku z powyższymi ustaleniami została przeprowadzona kontrola w Poltransplancie, której zakresem objęto m.in. ustalenie podstawy prawnej przekazywania przez Poltransplant do działających ośrodków dawców szpiku, danych osobowych potencjalnych dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej pozyskanych przez podmioty, które następnie nie otrzymały zezwoleń Ministra Zdrowia na prowadzenie działalności ośrodka dawców szpiku, a także ustalenie, czy wobec osób, których ww. dane dotyczyły, realizowany był obowiązek informacyjny, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych. W wyniku ww. kontroli ustalono, iż z dniem 15 września 2009 r., tj. z dniem wejścia w życie znowelizowanej ustawy transplantacyjnej, ośrodki dawców szpiku, które wcześniej prowadziły rejestry potencjalnych dawców, zostały zobowiązane do przekazywania danych potencjalnych dawców szpiku do Centralnego Rejestru prowadzonego przez Poltransplant. Podmioty prowadzące rejestry uzyskały status ośrodków dawców szpiku i przetwarzały dane osobowe (w systemach informatycznych i w postaci dokumentacji papierowej) potencjalnych dawców szpiku, którzy figurowali w prowadzonych przez nich rejestrach. W nowym systemie dawstwa szpiku w Polsce to ośrodki dawców, a nie Poltransplant, są podmiotami kontaktującymi się bezpośrednio z dawcami. Dlatego dokumentacja dotycząca dawców pochodząca z rejestru prowadzonego przez Poltransplant (oznaczonego PL5), została przekazana do ośrodków rekrutujących dla PL5, które stały się ośrodkami dawców szpiku. Natomiast pozostała dokumentacja została rozdzielona pomiędzy powstałe ośrodki dawców szpiku, z uwzględnieniem odległości od miejsca zamieszkania dawców lub preferencji wynikających z dotychczasowych zasad współpracy między tymi podmiotami. Poltrasplant podjął decyzję o ww. podziale dokumentacji dawców w uzgodnieniu z Ministerstwem Zdrowia w celu zapewnienie ciągłości i skuteczności pracy Centralnego Rejestru, gdyż przepisy obowiązującej ustawy transplantacyjnej nie zawierają rozstrzygnięć w kwestii danych potencjalnych dawców zebranych przed wejściem w życie regulacji prawnych dotyczących działalności ośrodków dawców szpiku.

Powyższe działania Poltransplantu uznane zostały za zasadne. Stwierdzono bowiem, że przekazanie przez Poltransplant do działających ośrodków dawców szpiku danych osobowych potencjalnych dawców pozyskanych przez inne podmioty w poprzednim stanie prawnym, było niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez odbiorców i administratorów danych oraz nie naruszało praw i wolności osób, których dane te dotyczyły. Zatem

---

<sup>40</sup> Art. 25. 1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, 3) źródle danych, 4) prawie dostępu do treści swoich danych oraz ich poprawiania, 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

podstawę legitymizującą takie działanie Poltransplantu stanowił art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych<sup>41</sup>.

Odnosząc się natomiast do kwestii realizacji obowiązku informacyjnego przez ww. podmiot oraz ośrodki dawców szpiku, którym przekazał on dane potencjalnych dawców, należy wskazać, że w toku kontroli przeprowadzonej w Poltransplancie ustalono, że wskazany obowiązek nie był realizowany z uwagi na skalę i koszt takiego przedsięwzięcia. Należy jednak zauważyć, iż w myśl art. 25 ust. 2 pkt 5 ustawy o ochronie danych osobowych, przepisu ust. 1 nie stosuje się, jeżeli dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1 (organ państwowy, organ samorządu terytorialnego, państwową lub komunalną jednostkę organizacyjną, podmiot niepubliczny realizujący zadania publiczne), na podstawie przepisów prawa. Tym samym Poltransplant nie miał obowiązku realizacji wobec ww. potencjalnych dawców obowiązku, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych. Na tej samej podstawie uznano, iż ośrodki dawców szpiku, które otrzymały dane osobowe dawców zrekrutowanych przez inne podmioty (prowadzące rejestry przed nowelizacją przepisów) także spełniają przesłanki do zwolnienia z dopełnienia obowiązku informacyjnego, jako podmioty, o których mowa w art. 3 ust. 1 i ust. 2 pkt 1 ustawy o ochronie danych osobowych (np. państwowe jednostki organizacyjne).

W toku kontroli badana też była kwestia przekazywania danych do europejskich i światowych rejestrów szpiku i krwi pępowinowej. Zgodnie z art. 38 ust. 3 pkt 14 ustawy transplantacyjnej, przekazywanie danych gromadzonych w „Centralnym rejestrze niespokrewnionych potencjalnych dawców szpiku i krwi pępowinowej” do europejskich i światowych rejestrów szpiku i krwi pępowinowej należy do zadań Poltransplantu. Tymczasem ustalono, że fundacja - będąca ośrodkiem dawców szpiku - przekazała dotychczas do Poltransplantu jedynie około 5 tys. rekordów z ogólnej liczby około 240 tys. zarejestrowanych przez tę fundację potencjalnych dawców. Nieprzekazanie całej bazy danych potencjalnych dawców wynikało z faktu, iż wciąż trwają prace w Poltransplancie mające na celu przygotowanie systemu informatycznego umożliwiającego przekazanie tych danych. Jednocześnie jednak ustalono, iż dane w zakresie: nr dawcy, wiek, płeć, oznaczenia HLA (zgodności tkankowej) były przekazywane przez tę fundację do niemieckiego centralnego rejestru dawców szpiku, za pośrednictwem którego dane te były następnie transferowane do ogólnoświatowego rejestru potencjalnych dawców szpiku. Udostępnienie danych do ww. rejestrów odbywało się na podstawie pozyskiwanej przez fundację zgody potencjalnych dawców na przekazywanie ich danych, w tym wyników przeprowadzonych analiz, do narodowych i międzynarodowych rejestrów w formie anonimowej. W przypadku, gdy potencjalny dawca poinformował fundację o rezygnacji z bycia dawcą,

---

<sup>41</sup> Art. 23. 1. 5. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

jego dane były usuwane z rejestrów. Ponadto na podstawie ww. zgody, kontrolowana fundacja planowała przekazywać dane potencjalnych dawców w wyżej wskazanym zakresie także do amerykańskiego rejestru dawców szpiku. W związku z tymi planami fundacja nie wystąpiła jeszcze do Generalnego Inspektora Ochrony Danych Osobowych o zgodę na przekazanie tych danych. Skierowała natomiast pismo z pytaniem „*czy (...) musi wystąpić do Generalnego Inspektora Ochrony Danych Osobowych z wnioskiem o wyrażenie zgody na przekazywanie anonimowych danych medycznych dawców zarejestrowanych w Fundacji (są to dane w postaci oznaczenia Typizacji HLA, numeru dawcy, wieku i płci dawcy) do położonego na terenie Stanów Zjednoczonych Ameryki Północnej, rejestru (...), tj. czy w opisanym powyżej stanie faktycznym, Fundacja (...) musi uzyskać zgodę Generalnego Inspektora Ochrony Danych Osobowych, o której mowa w art. 48 Ustawy?*”. Należy zauważyć, iż w toku kontroli fundacja stała na stanowisku, iż dane przekazywane przez nią do innych rejestrów nie są danymi osobowymi, gdyż nie pozwalają podmiotom prowadzącym te rejestry na identyfikację potencjalnego dawcy.

Z uwagi na to, iż działania fundacji budziły wątpliwości co do zgodności z przepisami ustawy transplantacyjnej, zakresem kontroli przeprowadzonej w Poltransplancie objęto także ustalenie, czy fundacja ta wypełniała prawidłowo wobec ww. podmiotu obowiązki nałożone na ośrodki dawców szpiku ustawą 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.). W szczególności, czy przekazała dane osobowe potencjalnych dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej do „Centralnego rejestru niespokrewnionych potencjalnych dawców szpiku i krwi pępowinowej”, a jeżeli nie to: 1) ustalenie przyczyny takiego stanu rzeczy, 2) ustalenie przewidywanego terminu przekazania tych danych przez fundację do wskazanego powyżej rejestru. Kontrola potwierdziła, że fundacja, jako ośrodek dawców szpiku, nie dopełniła obowiązku niezwłocznego przekazywania danych osobowych potencjalnych dawców do Centralnego Rejestru prowadzonego przez Poltransplant, zatem w tym zakresie zostanie wszczęte wobec niej postępowanie administracyjne.

Niezależnie od powyższego Generalny Inspektor wystąpił do Ministra Zdrowia - jako podmiotu odpowiedzialnego za nadzór nad stosowaniem przepisów ustawy transplantacyjnej - o wydanie opinii, czy w jego ocenie przekazywanie przez ośrodek dawców szpiku danych osobowych potencjalnych dawców do innych, niż Centralny Rejestr, rejestrów potencjalnych dawców szpiku, było dopuszczalne w świetle przepisów ustawy transplantacyjnej, przy założeniu, iż uprzednio osoba, której dane dotyczą, wyraziła zgodę na ich przekazanie.

W toku przeprowadzonych kontroli stwierdzano także inne niż wyżej opisane uchybienia w procesie przetwarzania danych osobowych. Dotyczyły one m.in. powierzenia przez jeden z ośrodków dawców szpiku, w związku z realizacją zadania o którym mowa w art. 16a ust. 2 pkt 3

ustawy transplantacyjnej<sup>42</sup>, przetwarzania danych osobowych potencjalnych dawców podmiotowi prywatnemu świadczącemu tzw. „usługi outsourcingowe”, na podstawie zawartej na piśmie umowy. W związku z tym ustaleniem Generalny Inspektor zwrócił się do ośrodka dawców szpiku o złożenie wyjaśnień poprzez wskazanie, czy w skontrolowanym ośrodku oraz w ww. podmiocie, któremu powierzono przetwarzanie danych osobowych potencjalnych dawców szpiku lub komórek macierzystych, dostęp do przedmiotowych danych posiadają wyłącznie osoby o kwalifikacjach wskazanych w art. 16a ust. 4 ustawy transplantacyjnej<sup>43</sup>. W odpowiedzi wskazano jedynie, iż osoba kierująca ośrodkiem dawców szpiku jest specjalistą z zakresu hematologii, zaś dyrektor podmiotu prowadzącego ośrodek dawców szpiku jest specjalistą z zakresu biotechnologii. Nie udzielono natomiast odpowiedzi na pytanie, czy pozostali pracownicy ośrodka dawców szpiku posiadający dostęp do danych potencjalnych dawców spełniają powyższe wymagania, jak również, czy w podmiocie, któremu powierzono przetwarzanie danych osobowych potencjalnych dawców, dostęp do przedmiotowych danych posiadają wyłącznie osoby o kwalifikacjach wskazanych w przytoczonym powyżej przepisie. Zatem w niniejszej sprawie ośrodek dawców szpiku nie przedstawił dowodów, z których wynikałoby, iż właściwie wypełnił obowiązek wskazany art. 16a ust. 4 ustawy transplantacyjnej, który dotyczy nie tylko osób zajmujących kierownicze stanowiska w ośrodku dawców szpiku, lecz wszystkich osób, które w związku z realizacją jego zadań posiadają dostęp do tych danych.

W dwóch ośrodkach dawców szpiku nie zapewniono, aby dane osobowe były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. W jednym z ww. ośrodków ustalono, iż dane osób, które nie zostały zakwalifikowane na potencjalnych dawców, były również wpisane do prowadzonej przez ten ośrodek bazy danych, ale nie został im nadany status „dawca aktywny”, lecz zamieszczano przy nich jedynie adnotację o dyskwalifikacji z powodów zdrowotnych. Dane takiej osoby zostały wprowadzane w celu uniknięcia ponownej rejestracji takiej osoby przez inny ośrodek dawców szpiku. Mając na uwadze brzmienie art. 16a ust. 9 ustawy transplantacyjnej<sup>44</sup>, powyższą praktykę uznano za nieuzasadnioną. Dane tych osób nie powinny być umieszczane w centralnym rejestrze niespokrewnionych potencjalnych dawców szpiku i krwi pępowinowej, bowiem ustał cel, dla którego dane te zostały zebrane (rekrutacja potencjalnych dawców szpiku).

---

<sup>42</sup> Art. 16a. 2. 3. Do zadań ośrodka dawców szpiku należy w szczególności przechowywanie danych, o których mowa w ust. 8, i ich aktualizacja z uwzględnieniem możliwości ich przechowywania w formie elektronicznej.

<sup>43</sup> Art. 16a. 4. Zadania, o których mowa w ust. 2, wykonują osoby, które posiadają wykształcenie medyczne, biologiczne lub biotechnologiczne i odbyły szkolenie, o którym mowa w art. 40a ust. 1 ustawy transplantacyjnej.

<sup>44</sup> Art. 16a. 9. Ośrodek dawców szpiku przechowuje dokumentację potencjalnych dawców szpiku i komórek krwiotwórczych krwi obwodowej przez co najmniej 30 lat od dnia założenia dokumentacji potencjalnego dawcy szpiku i komórek krwiotwórczych krwi obwodowej, w sposób umożliwiający identyfikację potencjalnego dawcy szpiku i komórek krwiotwórczych krwi obwodowej.

W drugim z ośrodków dawców szpiku ustalono natomiast, iż w sytuacji, gdy osoba zgłaszająca się do ośrodka nie zakwalifikowała się jako potencjalny dawca, to jej dokumentacja była nadal przechowywana jako dokumentacja archiwalna (tym osobom nie nadawano nr Poltransplantu PL5-ID), zaś dane nie były usuwane z systemu informatycznego, tylko oznaczano je kolorem czerwonym. Jak ustalono, dane osobowe dotyczące takich osób były przechowywane ze względów bezpieczeństwa, m.in. wirusologicznego i bakteriologicznego. Przetwarzanie danych osób, które nie zostały zakwalifikowane jako potencjalni dawcy uznano jednak za nieuzasadnione. Nie podlega dyskusji, iż dane te były pozyskiwane w związku z realizacją zadania nałożonego na ośrodki dawców szpiku, o którym mowa w przepisach ustawy transplantacyjnej. Jednakże do dokumentacji zawierającej dane ww. osób nie mają zastosowania przepisy art. 16a ust. 9 ww. ustawy, gdyż osoby te nigdy nie stały się potencjalnymi dawcami (zostały one zdyskwalifikowane jako potencjalni dawcy szpiku i komórek macierzystych krwi). Zatem z chwilą ustalenia, iż osoba, która zgłosiła się do ośrodka nie może zostać zarejestrowana jako potencjalny dawca, jej dane powinny zostać usunięte, gdyż ustał cel, dla którego zostały pozyskane.

Kontrola przeprowadzona w innym ośrodku dawców szpiku wykazała, że ośrodek ten współpracuje z ośrodkami zagranicznymi przeprowadzającymi badania materiału pobranego od potencjalnych dawców szpiku. W związku z powyższym dochodziło do powierzenia przetwarzania danych osobowych ww. osób tym ośrodkom. Ośrodek ten nie zawarł jednak z ww. ośrodkami zagranicznymi umowy na piśmie określającej co najmniej zakres danych powierzonych im do przetwarzania i cel ich przetwarzania, co było spowodowane stanowiskiem przyjętym przez ten ośrodek, iż nie przekazuje do ww. podmiotów danych osobowych potencjalnych dawców, lecz jedynie zakodowany (oznaczony indywidualnym numerem dawcy) materiał genetyczny w postaci próbki krwi lub pałeczek z pobranym wymazem z jamy ustnej w celu przeprowadzenia badań. Każdej osobie, która chciała zostać zarejestrowana jako potencjalny dawca szpiku, nadawany był indywidualny (i niepowtarzalny) numer dawcy. Numer ten znajdował się w szczególności na formularzu rejestracyjnym wypełnianym przez ww. osoby i wprowadzany był do systemu informatycznego wykorzystywanego przez ośrodek dawców szpiku do przetwarzania danych osobowych potencjalnych dawców, a także były nim oznaczane wszelkie próbki z materiałem przeznaczonym do badań. Numer ten ośrodek dawców szpiku może bez nadmiernych kosztów, czasu i działań powiązać z innymi informacjami dotyczącymi potencjalnych dawców, które zostały zebrane w związku z wypełnieniem przez te osoby formularza rejestracyjnego oraz wprowadzeniem tych informacji do systemu informatycznego ośrodka. Wynika z tego, że dla ośrodka dawców szpiku numer dawcy był jedną z tych informacji, na podstawie których identyfikował on potencjalnych dawców szpiku zarejestrowanych w prowadzonej przez nią bazie danych. Skoro zatem poprzez ten numer ośrodek był w stanie zidentyfikować konkretną osobę, to należy uznać, że stanowi on dane osobowe w rozumieniu art. 6

ustawy o ochronie danych osobowych<sup>45</sup>. Należy także zauważyć, że w art. 6 ust. 2 ww. ustawy o ochronie danych osobowych wprost zostało wskazane, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić w szczególności poprzez powołanie się na numer identyfikacyjny. Nadawany przez ośrodek dawców szpiku każdemu potencjalnemu dawcy szpiku indywidualny (i niepowtarzalny) numer dawcy, miał niewątpliwie charakter numeru identyfikacyjnego, o którym mowa w powołanym przepisie ustawy o ochronie danych osobowych. Zatem z uwagi na fakt, że numer dawcy stanowi dane osobowe uznano, że z przekazaniem materiału do badań związane było przekazanie ośrodkom je wykonującym danych osobowych potencjalnych dawców szpiku. Dla słuszności powyższego stanowiska nie miał znaczenia fakt, że podmiot, który dane otrzymał, na podstawie numeru dawcy nie mógł ustalić tożsamości konkretnej osoby. Przy ocenie bowiem, czy określone informacje stanowią dane osobowe istotne jest wyłącznie to, czy te informacje są danymi osobowymi dla administratora danych. A jak wyżej wskazano, dla ośrodka dawców szpiku numer dawcy stanowił dane osobowe. W konsekwencji należy stwierdzić, że nawiązując współpracę z ośrodkami przeprowadzającymi badania materiału pobranego od potencjalnych dawców szpiku, skutkującą przekazaniem im danych osobowych ww. osób, ośrodek dawców szpiku powinien zapewnić, aby przekazanie tych danych następowało zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych, tj. w oparciu o umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych<sup>46</sup>, określającą zakres i cel przetwarzania przez taki ośrodek powierzonych danych osobowych oraz przy uwzględnieniu wymogów związanych z przekazywaniem danych do państwa trzeciego, w przypadku współpracy z ośrodkiem mającym siedzibę w takim państwie.

Do częstych uchybień stwierdzanych w toku kontroli należało również niedokonywanie aktualizacji informacji zawartych w zgłoszonym Generalnemu Inspektorowi do rejestracji zbiorze danych osobowych. Na podstawie wyników kontroli w zakresie stwierdzonych uchybień wobec odpowiedzialnych za nie ośrodków dawców szpiku zostały wszczęte postępowania administracyjne.

---

<sup>45</sup> 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.

<sup>46</sup> 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.



## 2.2.7. Szkolnictwo wyższe

W analizowanym 2012 r. skontrolowano **10 podmiotów** należących do tego sektora - Ministerstwo Nauki i Szkolnictwa Wyższego<sup>47</sup>, osiem uczelni<sup>48</sup> oraz Ośrodek Przetwarzania Informacji Instytut Badawczy<sup>49</sup>. Zakresem kontroli objęto przetwarzanie danych osobowych studentów, doktorów, doktorów habilitowanych oraz nauczycieli akademickich i pracowników naukowych w Systemie Informacji o Szkolnictwie Wyższym, o którym mowa w art. 34a ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. Nr 164, poz. 1365 z późn. zm.).

System Informacji o Szkolnictwie Wyższym, obsługiwany przez system informatyczny o nazwie „POL-on”, miał służyć do stworzenia bazy danych zawierającej informacje o jednostkach naukowych i nauce polskiej. Gromadzone dzięki niemu informacje mają wspierać procesy decyzyjne Ministra Nauki i Szkolnictwa Wyższego odnośnie uczelni wyższych. Znajdują się w nim wszelkie dane o wszystkich polskich jednostkach naukowych, do których publiczny dostęp wynika z ustaw, a także rozporządzeń wydanych przez Ministra Nauki i Szkolnictwa Wyższego: rejestry szkół wyższych, informacje o kierunkach i profilach kształcenia, dane liczbowe dotyczące studentów, pracowników naukowych i wiele innych. W systemie dostępna jest również baza publikacji naukowych oraz wskaźniki ewaluacji szkół wyższych.

W myśl art. 34a ust. 1 ustawy Prawo o szkolnictwie wyższym, minister właściwy do spraw szkolnictwa wyższego (obecnie: Minister Nauki i Szkolnictwa Wyższego), prowadzi System Informacji o Szkolnictwie Wyższym przy użyciu systemu „POL-on”, obejmujący dane, o których mowa w art. 35 ust. 1 i 2 oraz ust. 3 pkt 2 i 3 ww. ustawy (m.in. roczne sprawozdanie z działalności uczelni) oraz wykazy, o których mowa w art. 129a (wykaz nauczycieli akademickich i pracowników naukowych) i art. 170c tej ustawy (wykaz studentów). Ponadto do ww. systemu wprowadzane są dane osobowe doktorów oraz doktorów habilitowanych, na podstawie § 29 ust. 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 22 września 2011 r. w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodach doktorskich, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora (Dz. U. Nr 204, poz. 1200).

W toku przedmiotowych kontroli ustalono, że do ww. systemu za pośrednictwem strony internetowej wprowadzane były dane osobowe studentów, doktorów, doktorów habilitowanych oraz nauczycieli akademickich i pracowników naukowych. Dane osobowe przesyłane do systemu POL-on przetwarzane były na serwerach będących własnością Ośrodka Przetwarzania Informacji Instytutu Badawczego (dalej: OPI). OPI przetwarzało ww. dane na podstawie umowy powierzenia przetwarzania danych osobowych zawartej z Ministrem Nauki i Szkolnictwa Wyższego.

---

<sup>47</sup> DIS-K-421/144/12

<sup>48</sup> Np. kontrole: DIS-K-421/150/12, , DIS-K-421/145/12, DIS-K-421/136/12, DIS-K-421/129/12.

<sup>49</sup> DIS-K-421/166/12

Ośrodek Przetwarzania Informacji jest podmiotem odpowiedzialnym za tworzenie, utrzymanie baz danych i zarządzanie administracyjnym systemem informatycznym w ramach projektu realizowanego w celu wykonania obowiązków nałożonych przez Ministra Nauki i Szkolnictwa Wyższego w art. 35 ust. 1 i ust. 3 pkt 2 i pkt 3, art. 129a, art. 170c ustawy Prawo o szkolnictwie wyższym oraz § 29 ust. 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodach doktorskich, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora. Za zabezpieczenie danych osobowych przekazanych do Ministerstwa Nauki i Szkolnictwa Wyższego odpowiada OPI, na podstawie zawartych umów.

W toku przeprowadzonych kontroli pojawiły się wątpliwości w przedmiocie podstaw prawnych przetwarzania w systemie POL-on danych osobowych, które nie wynikają wprost z przepisów prawa, takich jak drugie imię oraz kraj wydania dokumentu tożsamości.

W toku kontroli wskazano, iż przetwarzanie w systemie POL-on danej dotyczącej drugiego imienia (jeżeli osoba je posiadała) było niezbędne z uwagi na zachowanie tożsamości danych przetwarzanych w bazie uczelni z danymi przetwarzanymi w systemie POL-on. Tym samym imię, o którym mowa w ustawie Prawo o szkolnictwie wyższym, było rozumiane jako całość informacji o imieniu, tj. danymi zawartymi w bazie uczelnianej. Ponadto system POL-on musiał uwzględniać dane zawarte w dokumencie tożsamości. W przeciwnym wypadku mogło dojść do błędów w identyfikacji osób.

W sytuacji przetwarzania przez Ministra Nauki i Szkolnictwa Wyższego w systemie POL-on informacji dotyczącej kraju wydania dokumentu tożsamości osoby, której nie nadano nr PESEL, podstawę prawną takiego przetwarzania stanowił art. 43 ust. 6b ustawy Prawo o szkolnictwie wyższym. Zgodnie z powołanym przepisem rektor przekazuje ministrowi właściwemu do spraw szkolnictwa wyższego, w terminie do 15 stycznia każdego roku, wykazy cudzoziemców, o których mowa w ust. 3 i 4, sporządzone według stanu na dzień 31 grudnia poprzedniego roku, ze wskazaniem osób posiadających Kartę Polaka lub spełniających wymagania określone w art. 5 ust. 1-3 ustawy z dnia 9 listopada 2000 r. o repatriacji, zawierające: imię i nazwisko cudzoziemca, państwo zamieszkania, kierunek i rok studiów lub inny rodzaj kształcenia oraz jednostkę organizacyjną uczelni, w której cudzoziemiec odbywa kształcenie, a także warunki finansowe kształcenia. Wskazano ponadto, iż przetwarzanie danej dotyczącej kraju wydania dokumentu potwierdzającego tożsamość osoby było niezbędne z uwagi na to, iż dana ta jest nierozłącznie powiązana z numerem dokumentu tożsamości.

Analiza przepisów prawa wykazała, iż zakres danych osobowych, jaki może być zamieszczony w systemie informatycznym o nazwie „POL-on”, stanowił katalog zamknięty, szczegółowo określony przez przepisy prawa, tj. art. 129a ust. 1 (wykaz nauczycieli akademickich i pracowników naukowych) i art. 170c ust. 2 ustawy Prawo o szkolnictwie wyższym (wykaz studentów). Biorąc pod uwagę

powyższe Minister Nauki i Szkolnictwa Wyższego winien uwzględnić ww. dane osobowe w przyszłych pracach legislacyjnych dotyczących ustawy Prawo o szkolnictwie wyższym.

Pojawiły się też wątpliwości w przedmiocie przetwarzania w Systemie Informacji o Szkolnictwie Wyższym przy użyciu systemu informatycznego o nazwie „POL-on”, danych osobowych doktorów i doktorów habilitowanych.

Podstawą prawną przetwarzania danych osobowych doktorów i doktorów habilitowanych w systemie POL-on jest art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, tj. przetwarzanie danych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Przepisem tym jest § 29 ust. 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodach doktorskich, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora, wydanego na podstawie art. 31 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. Nr 65, poz. 595 z późn. zm.). Zgodnie z § 29 ust. 1 powołanego rozporządzenia, nazwiska osób, którym nadano stopień doktora lub doktora habilitowanego, ogłasza się w dzienniku urzędowym ministra właściwego do spraw szkolnictwa wyższego na podstawie zawiadomień przesyłanych w formie elektronicznej przez kierowników jednostek organizacyjnych. Wobec powyższego wskazać należy, iż z przepisów tych nie wynika, iż dane osobowe doktorów i doktorów habilitowanych zamieszcza się w Systemie Informacji o Szkolnictwie Wyższym. Zatem Minister Nauki i Szkolnictwa Wyższego powinien również uwzględnić i te wymienione powyżej wątpliwości w przyszłych pracach legislacyjnych dotyczących ustawy Prawo o szkolnictwie wyższym.

W toku czynności kontrolnych przeprowadzonych w uczelniach nie było możliwości ustalenia, czy w odniesieniu do danych osobowych dotyczących pracowników naukowych i nauczycieli akademickich system informatyczny o nazwie „POL-on” spełniał wymogi przepisów o ochronie danych osobowych w zakresie § 7 ust. 1 pkt 1 i pkt 2 oraz § 7 ust. 3 rozporządzenia<sup>50</sup>. Osoby administrujące systemem POL-on na poziomie uczelni nie posiadały bowiem dostatecznej wiedzy w tym zakresie i nie były w stanie udokumentować wymaganej funkcjonalności systemu POL-on.

Mając na uwadze powyższe Generalny Inspektor wystąpił do Ministra Nauki i Szkolnictwa Wyższego wskazując, iż powinien on przekazywać uczelniom dokumentację, która zawierałaby pełny opis funkcjonalności systemu POL-on, a także przeprowadzał szkolenia dla użytkowników systemu

---

<sup>50</sup> § 7. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie: 1) daty pierwszego wprowadzenia danych do systemu; 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba. § 7. 3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

POL-on, co będzie stanowiło realizację obowiązków nałożonych na administratora danych przez przepis art. 36 ust. 1 ustawy<sup>51</sup>.

Najczęściej nieprawidłowości stwierdzone w toku kontroli w uczelniach polegały na nieprowadzeniu dokumentacji opisującej sposób przetwarzania danych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (art. 36 ust. 2 ustawy o ochronie danych osobowych). W dwóch podmiotach polityka bezpieczeństwa nie zawierała informacji dotyczących systemu informatycznego o nazwie „POL-on”, zaś w jednej uczelni z kolei instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych nie zawierała tej informacji. W jednym z podmiotów nie został wyznaczony administrator bezpieczeństwa informacji (art. 36 ust. 3 ustawy o ochronie danych osobowych), w innym nie zapewniono, aby zmiana hasła do systemu informatycznego o nazwie POL-on następowała nie rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych) oraz nie został dopełniony obowiązek aktualizacji zbiorów danych. W jednej z uczelni stwierdzono nieprawidłowości polegające na tym, iż dane dotyczące nauczycieli akademickich nie były przekazywane do systemu POL-on, aktualizowane i odznaczane jako archiwalne w terminach 7 dniowych, tj. niedopełniono obowiązku wynikającego z § 5 i § 6 ust. 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 29 września 2011 r. w sprawie centralnego wykazu nauczycieli akademickich i pracowników naukowych.

W Ośrodku Przetwarzania Informacji nie stwierdzono uchybień w zakresie objętym kontrolą.

Na podstawie wyników kontroli prowadzone były postępowania administracyjne w celu przywrócenia stanu zgodnego z prawem. Ponadto skierowano wystąpienie do Ministra Nauki i Szkolnictwa Wyższego w przedmiocie uwzględnienia uwag dotyczących zakresu danych osobowych przetwarzanych w systemie POL-on podczas nowelizacji przepisów dotyczących Systemu Informacji o Szkolnictwie Wyższym, o którym mowa w art. 34a ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. Nr 164, poz. 1365 z późn. zm.).

---

<sup>51</sup> Art. 36.1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

### 2.2.8. Usługi hotelarskie

W okresie sprawozdawczym przeprowadzono **11 kontroli** zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w podmiotach prowadzących hotele<sup>52</sup>. Zakresem kontroli objęto przetwarzanie przez ww. podmioty danych osobowych osób korzystających z usług hotelarskich.

W toku kontroli ustalono, iż niektórzy przedsiębiorcy prowadzący hotele zarządzają hotelami własnymi, pozostali zaś zarządzają hotelami na podstawie zawartych umów o zarządzanie lub franczyzę. W przypadku hoteli działających na podstawie umów o zarządzanie, stronami zawartych umów były dwa podmioty, tj. spółka będąca właścicielem znaku handlowego, jak również podmiot, do którego należy przedsiębiorstwo hotelowe. W tego typu umowach podmiot będący właścicielem przedsiębiorstwa hotelowego uzgadnia z podmiotem, do którego należy znak handlowy, warunki korzystania z tego znaku oraz warunki zarządzania przedsiębiorstwem. W przypadku takiej działalności zarządzanie obejmuje również wdrożenie i stosowanie systemu informatycznego służącego do przetwarzania danych osobowych osób korzystających z usług hotelowych. Natomiast w sytuacji zarządzania hotelami objętymi umową franczyzy, na podstawie zawartej umowy spółka będąca właścicielem znaku handlowego, zezwala lub umożliwia podmiotowi, do którego należy przedsiębiorstwo hotelowe, na korzystanie z jej znaku. W takich przypadkach podmiot, do którego należy przedsiębiorstwo hotelowe, całkowicie kieruje i zarządza przedsiębiorstwem hotelowym, korzystając wyłącznie ze standardów wynikających ze znaku handlowego. Przedsiębiorcy prowadzący hotele świadczą usługi hotelarskie w zakresie krótkotrwałego wynajmu pokoi, o którym mowa w art. 3 pkt 8 ww. ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (tj. Dz. U. z 2004 r. Nr 223, poz. 2268 z późn. zm.).

Oceniając wyniki przeprowadzonych kontroli stwierdzić należy, iż najwięcej zastrzeżeń w procesie przetwarzania danych osobowych wzbudzało niedopełnienie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych<sup>53</sup>. Wskazać bowiem należy, iż przedsiębiorcy prowadzący hotele jako administratorzy danych osób korzystających z usług hotelarskich, najczęściej nie informowali osób rezerwujących usługi hotelarskie o adresie swojej siedziby i pełnej nazwie. Na podkreślenie zasługuje fakt, iż we wszystkich skontrolowanych podmiotach nazwa hotelu nie była tożsama z nazwą administratora danych. W niektórych przypadkach również adres hotelu nie był tożsamy z adresem siedziby administratora danych. Natomiast

---

<sup>52</sup> Np. kontrole DIS-K-421/42/12, DIS-K-421/46/12 i DIS-K-421/55/12.

<sup>53</sup> Art. 24. ust. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku, 2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, 3) prawie dostępu do treści swoich danych oraz ich poprawiania, 4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

w większości przypadków osoby korzystające z usług hoteli informowane były jedynie o adresie i siedzibie danego hotelu, natomiast nie informowano ich o nazwie administratora danych i adresie jego siedziby.

Ponadto liczne uchybienia dotyczyły niedopełnienia, wynikającego z art. 40 ustawy o ochronie danych osobowych<sup>54</sup>, obowiązku zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji prowadzonych zbiorów danych, dotyczących osób korzystających z usług hotelarskich. Natomiast w pojedynczych przypadkach stwierdzano nieprawidłowości polegające na przetwarzaniu danych osobowych w zakresie nieadekwatnym do celu, w jakim zostały zebrane (w związku z pozyskiwaniem danych dotyczących numeru paszportu na potrzeby prowadzonego programu lojalnościowego), nieokreśleniu terminu przechowywania danych osób, które dokonały anulowania rezerwacji pobytu w hotelu oraz terminu usuwania ze skrzynek poczty elektronicznej rezerwacji dokonanych drogą elektroniczną, a także nieopracowaniu procedur, które regulowałyby sposób działania archiwów prowadzonych w hotelach, w tym m.in. zasady przekazywania dokumentacji do archiwum i jej wypożyczania, a także okresy przechowywania dokumentacji w archiwum i jej niszczenia.

Przeprowadzone kontrole wykazały również uchybienia w procesie przetwarzania danych osobowych w systemach informatycznych. Dotyczyły one m.in. dokonywania zmiany haseł dostępu do systemu informatycznego rzadziej niż co 30 dni, używaniu do uwierzytelnienia hasła niezawierającego co najmniej 8 znaków oraz przesyłaniu za pośrednictwem strony internetowej danych osobowych w sposób niezabezpieczony protokołem szyfrującym https.

Większość kontroli wykazała, że przedsiębiorcy prowadzący hotele zastosowali środki techniczne i organizacyjne zapewniające ochronę danych osobowych przetwarzanych w systemie tradycyjnym (papierowym), odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności dane osobowe zostały zabezpieczone przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jedynie w kilku przypadkach stwierdzono w tym zakresie uchybienia, które dotyczyły przechowywania dokumentacji zawierającej dane osobowe na odkrytych półkach oraz w niezamykanych na klucz szafkach.

Na podstawie stwierdzonych w toku kontroli nieprawidłowości w procesie przetwarzania danych osobowych, wobec podmiotów winnych uchybień zostały wszczęte postępowania administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych. Postępowania te zostały zakończone wydaniem decyzji administracyjnych nakazujących usunięcie nieprawidłowości<sup>55</sup> oraz decyzji

---

<sup>54</sup> Art. 40. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

<sup>55</sup> Np. decyzja nr DIS/DEC-1177/12/72416.

umarzających postępowania<sup>56</sup>. W decyzjach tych Generalny Inspektor nakazywał m.in. dopełnienie obowiązku informacyjnego i zgłoszenie prowadzonego zbioru danych do rejestracji. Przesłanką umorzenia postępowania była ich bezprzedmiotowość spowodowana usunięciem uchybień w procesie przetwarzania danych osobowych w toku postępowania administracyjnego.

### 2.2.9. Inne

Istotne problemy w procesie przetwarzania danych osobowych stwierdzone były również w toku kontroli przeprowadzonych w podmiotach nienależących do żadnego z przedstawionych wyżej sektorów. Najczęściej kontrole te były wykonywane na zlecenie Departamentu Orzecznictwa Legislacji i Skarg oraz Departamentu Rejestracji Zbiorów Danych Osobowych Biura GODO. Ich ogólnym celem była weryfikacja zgodności przetwarzania danych osobowych z przepisami ustawy. Stałym elementem tej weryfikacji była kontrola zastosowanych przez administratorów danych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych. W wielu przypadkach weryfikacja ta dotyczyła również legalności przetwarzania, jak również zgodności, czy zastosowane rozwiązania techniczne nie powodują przekroczenia zakresu przetwarzania danych w stosunku do celu, któremu mogą służyć.

W grupie tej przeprowadzono **109 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Jedna z bardziej interesujących kontroli była przeprowadzona **w stowarzyszeniu**, w którym – w celu uproszczenia prowadzonej dokumentacji oraz cyfryzacji stowarzyszenia - rozpoczęto pracę nad zastąpieniem legitymacji i książeczek (potwierdzających m.in. członkostwo w stowarzyszeniu) kartami magnetycznymi z nadrukowanymi danymi w zakresie: imię, nazwisko, numer ewidencyjny i numer kodu kreskowego. Podstawową funkcją tych kart było potwierdzenie członkostwa w stowarzyszeniu, zaś dodatkowo karta pełniła funkcję płatniczą jako instrument pieniądza elektronicznego, tzw. „elektroniczna portmonetka”. W związku z wprowadzeniem kart członkowskich stowarzyszenie zawarło z jednym z banków umowę dotyczącą zasad współpracy wydawania i obsługi kart przedpłaconych. Przedmiotem ww. umowy było wydawanie przez bank na zlecenie stowarzyszenia kart przedpłaconych na okaziciela, jako instrumentu pieniądza elektronicznego w rozumieniu ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. z 2002, Nr 169, poz. 1385 z późn. zm.). Na podstawie tej umowy stowarzyszenie zamówiło w banku ponad 82 tys. kart przedpłaconych i zleciło mu nadrukowanie na nich informacji w zakresie: logo stowarzyszenia i jego pełna nazwa – karta członkowska oraz imion i nazwisk, a także numeru członkowskiego stowarzyszenia. Ponadto na karcie miały znaleźć się następujące informacje: numer karty, logo

---

<sup>56</sup> Np. decyzja nr DIS/DEC-2/13/73.

organizacji kartowej, logo banku oraz informacja o wystawcy karty – pełna nazwa i adres siedziby, a także adres strony internetowej banku. Każda osoba, która otrzymała nową kartę/legitymację członkowską otrzymała także regulamin karty przedpłaconej na okaziciela, wraz z informacjami na temat funkcjonalności karty. Zgodnie z ww. regulaminem, umowa o instrument pieniądza elektronicznego została zawarta w momencie pierwszego zasilenia karty i obowiązywała maksymalnie do upływu ważności karty. Zdaniem stowarzyszenia informacje, które zostały przekazywane do banku, w zakresie: logo stowarzyszenia i jego nazwa – karta członkowska oraz imię i nazwisko, jak również numer członkowski stowarzyszenia, nie są danymi osobowymi w rozumieniu przepisów ustawy o ochronie danych osobowych, gdyż na ich podstawie bank nie jest w stanie zidentyfikować osoby, której informacje te dotyczą. Ponadto ustalenie tożsamości i identyfikacja osoby na podstawie tych informacji wymagałaby poniesienia przez każdą osobę, w tym bank, nadmiernych kosztów, czasu i działań. Zdaniem stowarzyszenia nie doszło w tym przypadku do udostępnienia danych osobowych. Jednak z uwagi na treść art. 6 ustawy o ochronie danych osobowych<sup>57</sup>, Generalny Inspektor nie zgodził się ze stanowiskiem stowarzyszenia z uwagi na to, że na podstawie powyższych informacji istnieje możliwość zidentyfikowania osoby, której te dane dotyczą. Taką możliwość posiada nie tylko stowarzyszenie, ale także i bank, który może wystąpić do stowarzyszenia z prośbą o zidentyfikowanie osoby, której dane dotyczą. Istnieje zatem możliwość jednoznacznego zidentyfikowania danej osoby. Generalny Inspektor uznał w konsekwencji, iż informacje w zakresie imienia, nazwiska i numeru członkowskiego stowarzyszenia były danymi osobowymi w rozumieniu art. 6 ustawy o ochronie danych osobowych, a ustalenie tożsamości na podstawie tych danych nie wymagało od stowarzyszenia oraz banku, poniesienia nadmiernych kosztów, czasu lub działań.

Jednocześnie dla oceny sytuacji istotne było to, czy ww. dane zostały udostępnione, czy też zostały powierzone do przetwarzania bankowi, zgodnie z art. 31 ustawy o ochronie danych osobowych. W związku z powyższym przeprowadzono w banku współpracującym ze stowarzyszeniem kontrolę w zakresie przetwarzania danych osobowych członków stowarzyszenia w związku z wydawaniem legitymacji członkowskich stowarzyszenia oraz kart przedpłaconych. W toku kontroli ustalono, iż dane przekazane przez stowarzyszenie były przetwarzane przez bank w celach reklamacyjnych, np. w celu dokonania ponownego wydrukowania karty, w przypadku, gdy dane na karcie zostały wydrukowane niepoprawnie. Ww. dane nie były natomiast przetwarzane przez bank w celu obsługi kart przedpłaconych oraz w celu rejestracji tych kart w internetowym serwisie kart. Podstawą prawną przetwarzania przez bank danych osobowych członków stowarzyszenia była umowa dotycząca zasad

---

<sup>57</sup> 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.



wydawania i obsługi kart przedpłaconych, zawarta ze stowarzyszeniem. Jednocześnie jednak ustalono, że z chwilą otrzymania przez posiadacza/użytkownika ww. karty wraz z regulaminem, bank składał ofertę zawarcia umowy o instrument pieniądza elektronicznego. Zawarcie tej umowy następowało z chwilą pierwszego zasilenia karty, tj. przelania/wpłaty środków pieniężnych na rachunek techniczny, którego numer znajduje się na rewersie karty. Mając powyższe na uwadze Generalny Inspektor uznał, iż w związku z wprowadzeniem kart członkowskich stowarzyszenia wydanych przez bank, stowarzyszenie zaoferowało swoim członkom produkt marketingowy tego banku, tj. karty przedpłacone na okaziciela będące instrumentem pieniądza elektronicznego. Z chwilą otrzymania przez posiadacza/użytkownika ww. karty wraz z regulaminem karty przedpłaconej na okaziciela, bank składał mu bowiem ofertę zawarcia umowy o instrument pieniądza elektronicznego. Z uwagi na powyższe uznano, iż stowarzyszenie przetwarzało dane osobowe swoich członków w celach marketingowych produktów i usług innych podmiotów. Jednocześnie stowarzyszenie nie wskazało podstawy prawnej przetwarzania danych osobowych swoich członków w ww. celach. Uznano zatem, że przetwarzanie danych członków stowarzyszenia w tych celach odbywa się bez podstawy prawnej. Ustalono też, że umowa dotycząca zasad współpracy wydawania i obsługi kart przedpłaconych zawarta pomiędzy stowarzyszeniem a bankiem nie określała zakresu i celu powierzonych do przetwarzania danych. W tym zakresie wszczęte zostało postępowanie administracyjne.

W roku sprawozdawczym dokonano również czynności kontrolnych w **podmiotach przetwarzających dane osobowe użytkowników systemu wypożyczania rowerów o nazwie „Warszawski Rower Publiczny”<sup>58</sup>**. Istotnym elementem tych kontroli było ustalenie administratora danych osobowych użytkowników ww. systemu. W wyniku przeprowadzonych kontroli (m.in. w Urzędzie m.st. Warszawy) ustalono, że administratorem danych osobowych użytkowników systemu wypożyczania rowerów miejskich był jeden z podmiotów wchodzących w skład konsorcjum odpowiedzialnego za wdrożenie, zarządzanie i eksploatacją systemu. Podmiot ten zdecydował o tym, w jaki sposób i przy użyciu jakich środków usługa polegająca na uruchomieniu oraz zarządzaniu i kompleksowej eksploatacji systemu „Warszawski Rower Publiczny” będzie wykonana, w tym jaki będzie zakres i sposób przetwarzania danych osobowych użytkowników systemu wypożyczania rowerów miejskich. Ponadto podmiot ten zgłosił do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych osobowych, w ramach którego były przetwarzane dane osobowe użytkowników systemu wypożyczania rowerów miejskich z miast i gmin (organów administracji samorządowej), z którymi zawarte zostały umowy na świadczenie usługi polegającej na uruchomieniu oraz zarządzaniu i kompleksowej eksploatacji systemu wypożyczania rowerów miejskich.

---

<sup>58</sup> Kontrole DIS-K-421/110/12 i DIS-K-421/120/12.

Kolejny przykład dotyczył **kontroli przeprowadzonej na skutek korespondencji GIODO z czeskim organem ochrony danych osobowych w spółce prowadzącej portal internetowy w języku czeskim dla czeskich użytkowników**. W toku kontroli ustalono, że obowiązek informacyjny realizowany był w treści regulaminu oraz w polityce prywatności zamieszczonych w portalu (w języku czeskim), jednakże spółka nie przedstawiła wystarczających dowodów potwierdzających spełnienie obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych. Ustalono, że w zakresie wykorzystania infrastruktury technicznej oraz zasobów personalnych spółka zawarła umowę o świadczenie usług z innym podmiotem, który z kolei współpracował w zakresie dzierżawy serwera na podstawie umowy z kolejnym podmiotem. Umowy te dotyczyły ogólnych zasad współpracy pomiędzy ww. partnerami. Portal czeski został włączony do tych zasad, natomiast nie został on wprost wskazany w treści ww. umów. Należało zatem uznać, że przedmiotowe umowy nie dotyczyły powierzenia przetwarzania danych osobowych użytkowników czeskiego portalu, przez co doszło do naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 31 ust. 1 i ust. 2 ustawy o ochronie danych osobowych. W związku ze stwierdzonymi w spółce uchybieniami wydana została decyzja nakazująca spółce ich usunięcie<sup>59</sup>. Składając wniosek o ponowne rozpatrzenie sprawy spółka przedstawiła dowody potwierdzające spełnianie wobec użytkowników obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych. Z tych względów w decyzji ponownej uchylono nakaz dopełniania wobec użytkowników portalu ww. obowiązku i w tym zakresie postępowanie zostało umorzone, natomiast w pozostałym zakresie zaskarżona decyzja została utrzymana w mocy<sup>60</sup>.

Na uwagę zasługuje także **kontrola przeprowadzona w jednej z firm marketingowych**. Wykazała ona m.in., że osoby, których dane dotyczą, w celu udziału w loterii organizowanej przez ten podmiot, wypełniały formularz rejestracyjny i składały oświadczenie, w treści którego zawarta była zgoda na przetwarzanie danych osobowych w celach marketingowych oraz na otrzymywanie informacji handlowych drogą elektroniczną. Generalny Inspektor uznał, że zawarcie zgód na przetwarzanie danych osobowych w celach marketingowych oraz na otrzymywanie informacji handlowych drogą elektroniczną w treści jednego oświadczenia, bez jednoczesnego zapewnienia możliwości wyboru, oznaczało, że osoba, której dane dotyczyły, nie miała swobody w dysponowaniu swoimi danymi osobowymi, a w szczególności swobody w wyborze celów, w których jej dane miały być przetwarzane. Co prawda, jak ustalono, po kliknięciu na odnośnik „Pełna treść zgód: kliknij tutaj” znajdujący się w treści informacji dostępnej pod formularzem rejestracyjnym, otwierało się okno z czterema odrębnymi oświadczeniami o wyrażeniu zgody na przetwarzanie danych osobowych, to jednak nie było pewności, że każda osoba, która wypełniała formularz rejestracyjny, kliknie na ten

---

<sup>59</sup> Decyzja nr DIS/DEC-660/12/43788.

<sup>60</sup> Decyzja nr DIS/DEC-846/12/55103.

własnie odnośnik. Nie można więc było uznać, że w ten sposób zapewniona została przez administratora danych swoboda wyboru celów przetwarzania danych osobowych przez osoby, których one dotyczą. Niezbędne było bowiem umożliwienie osobie swobodnego wyrażenia woli w przedmiocie zgody na przetwarzanie dotyczących jej danych, np. poprzez zapewnienie opcjonalności w klauzuli zgody już przy pierwszym oświadczeniu odnoszącym się do wyrażania zgody na przetwarzanie jej danych, w szczególności wówczas, gdy dane te miały być przetwarzane w różnych celach. W związku z powyższym ustaleniem, wszczęte zostało wobec kontrolowanego administratora danych postępowanie administracyjne. W odpowiedzi administrator danych poinformował GODO o zamieszczeniu bezpośrednio pod formularzem rejestracyjnym odrębnych oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych tak, aby osobie składającej te oświadczenia zapewnić swobodę wyboru.

W toku kontroli przeprowadzonej **w jednej ze spółek prowadzącej sieć marketów spożywczo-przemysłowych** ustalono, że osoby ujęte na gorącym uczynku przestępstwa lub wykroczenia (kradzieży) w prowadzonych przez spółkę marketach, były proszone o przekazanie spółce danych personalnych w zakresie: imię, nazwisko, adres zamieszkania, numer dowodu osobistego lub paszportu, numer PESEL oraz data i miejsce urodzenia, w celu przygotowania zawiadomienia policji o zaistniałej kradzieży. Jak ustalono, ujęta osoba była informowana o tym, iż podanie danych osobowych jest dobrowolne i w związku z tym ma prawo odmówić ich podania i domagać się przekazania w ręce policji. W sytuacji, gdy osoba zdecydowała się przekazać spółce swoje dane osobowe, pracownik sklepu wprowadzał je do formularza o nazwie „Zawiadomienie o kradzieży”, w którym zamieszczał też opis zaistniałego zdarzenia oraz nazwy skradzionych przedmiotów i ich wartość. W toku kontroli ustalono, że dane osób schwytanych na gorącym uczynku przestępstwa lub wykroczenia (kradzieży) były przetwarzane w celu zawiadomienia policji o zaistniałej kradzieży, a ponadto dane te były wykorzystywane dla celów statystycznych (prowadzenia wewnętrznej ewidencji kradzieży w prowadzonych przez spółkę marketach). Jednocześnie w toku kontroli ustalono, że w spółce nie funkcjonowała wewnętrzna służba ochrony, o której mowa w ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 1997 r. Nr 114, poz. 740).

Mając na uwadze obowiązujące przepisy regulujące kwestię ujęcia obywatelskiego sprawcy przestępstwa lub wykroczenia<sup>61</sup>, Generalny Inspektor Ochrony Danych Osobowych zauważył, iż

---

<sup>61</sup> Art. 243 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.). Każdy ma prawo ująć osobę na gorącym uczynku przestępstwa lub w pościgu podjętym bezpośrednio po popełnieniu przestępstwa, jeżeli zachodzi obawa ukrycia się tej osoby lub nie można ustalić jej tożsamości. Art. 243 § 2 Kodeksu postępowania karnego. Osobę ujętą należy niezwłocznie oddać w ręce Policji. Art. 45 § 1 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (tekst jednolity: Dz. U. z 2008 r. Nr 133, poz. 848). Policja ma prawo zatrzymać osobę ujętą na gorącym uczynku popełnienia wykroczenia lub bezpośrednio potem, jeżeli: zachodzą podstawy do zastosowania wobec niej postępowania przyspieszonego: nie można ustalić jej tożsamości. Art. 45 § 2 Kodeksu postępowania w sprawach o wykroczenia. Art. 243 Kodeksu postępowania karnego stosuje się odpowiednio.

jednym z warunków legalnego ujęcia sprawcy przestępstwa lub wykroczenia jest niemożność ustalenia jego tożsamości. W związku z czym ujęcie sprawcy bez uprzedniego podjęcia próby ustalenia jego tożsamości, mogło w konsekwencji uniemożliwić osobie, która dokonała ujęcia, powołanie się na tę przesłankę. Zgodnie z poglądem doktryny<sup>62</sup> niemożność ustalenia sprawcy przestępstwa lub wykroczenia zachodzi w sytuacji, gdy sprawca nie jest znany osobie zatrzymującej go i nie posiada przy sobie dokumentów pozwalających na ustalenie jego tożsamości lub okazany przez niego dokument budzi wątpliwości co do jego wiarygodności. Warunek ten nie będzie spełniony, jeżeli osoba ujęta jest znana zatrzymującemu. W razie niespełnienia któregokolwiek z tych warunków, konieczne jest niezwłoczne uwolnienie sprawcy. Zatrzymanie sprawcy przestępstwa lub wykroczenia niespełniające wymogów art. 243 Kodeksu postępowania karnego, bezzasadne przetrzymywanie ujętego, może pociągać za sobą odpowiedzialność cywilną za wyrządzoną szkodę (art. 415 Kodeksu cywilnego<sup>63</sup>), a także odpowiedzialność karną z tytułu dopuszczenia się przestępstwa pozbawienia człowieka wolności (art. 189 Kodeksu karnego<sup>64</sup>).

W świetle powyższego Generalny Inspektor Ochrony Danych Osobowych uznał, iż pozyskiwanie przez spółkę od osób ujętych na gorącym uczynku przestępstwa lub wykroczenia (kradzieży) w prowadzonych przez spółkę marketach, danych osobowych w celu zawiadomienia policji o zaistniałej kradzieży, nie narusza obowiązujących przepisów.

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

W ramach przeprowadzonych w 2012 r. kontroli, weryfikacji poddano **280 systemów informatycznych**, tj. o 104 mniej niż w roku 2011, w którym skontrolowano 384 systemy informatyczne wykorzystywane 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

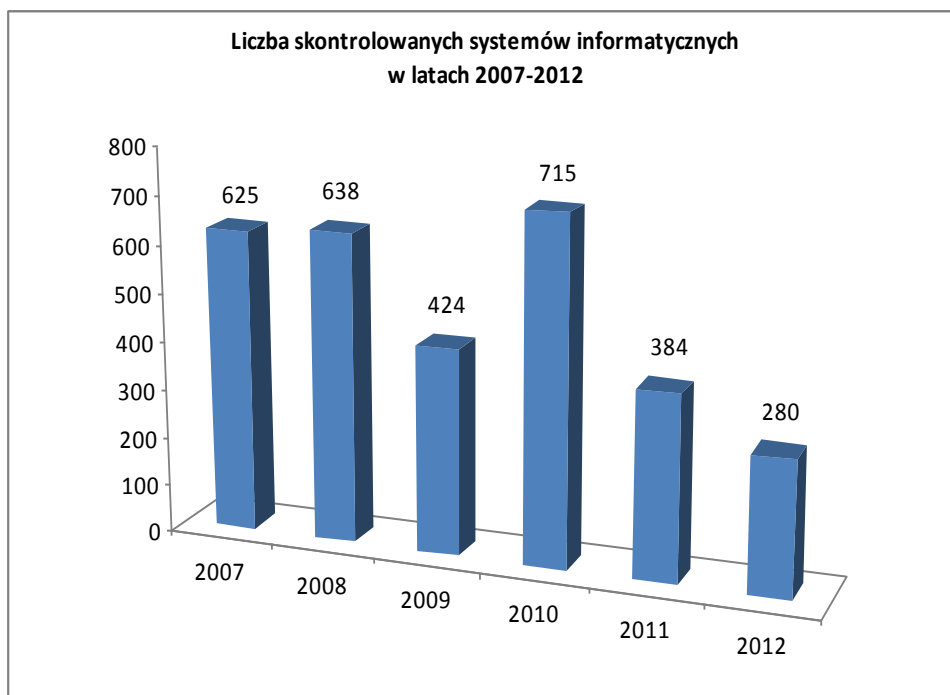
rok 2012 = 165 kontroli, obejmujących 280 systemów informatycznych

---

<sup>62</sup> J. Grajewski (red.), L. K. Paprzycki, S. Steiborn: Komentarz do art. 1-424 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego. System Informacji Prawnej Lex (Lex Omega) 34/2012; J. Bratoszewski, L. Gardocki, Z. Gostyński, S. M. Przyjemski, R. A. Stefański, S. Zabłocki: Kodeks postępowania karnego. Komentarz. System Informacji Prawnej Lex (Lex Omega) 34/2012.

<sup>63</sup> Art. 415 Kodeksu cywilnego: Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.

<sup>64</sup> Art. 189 § 1 Kodeksu karnego. Kto pozbawia człowieka wolności, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.



**Wykres 1: Zestawienie porównawcze liczby skontrolowanych systemów informatycznych w latach 2007-2012.**

Jak wynika z przedstawionego Wykresu 2, liczba systemów informatycznych objętych kontrolą w roku 2012 była niższa niż w latach poprzednich. Spowodowane to było tym, że większość z kontroli należało do kategorii tzw. kontroli częściowych, które swym zakresem obejmowały tylko wybrane zagadnienia dotyczące przetwarzania danych osobowych, np. obecności w przetwarzanych przez kontrolowany podmiot zbiorach danych informacji o określonej osobie, zastosowane zabezpieczenia, czy sposób przekazywania danych. Ponadto w toku kontroli systemów informatycznych wraz z weryfikacją stosowanych zabezpieczeń sprawdzana była również ich funkcjonalność w zakresie spełnienia warunków określonych w § 7 rozporządzenia, co jest jedną z najbardziej czasochłonnych operacji. Na mniejszą liczbę skontrolowanych systemów informatycznych miała również wpływ duża grupa kontroli sektorowych. Na przykład kontrole sektorowe banków i innych instytucji finansowych wykazały, że do przetwarzania danych osobowych używane były scentralizowane systemy informatyczne, zaś te przeprowadzane w podmiotach telekomunikacyjnych obejmowały swoim zakresem 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.

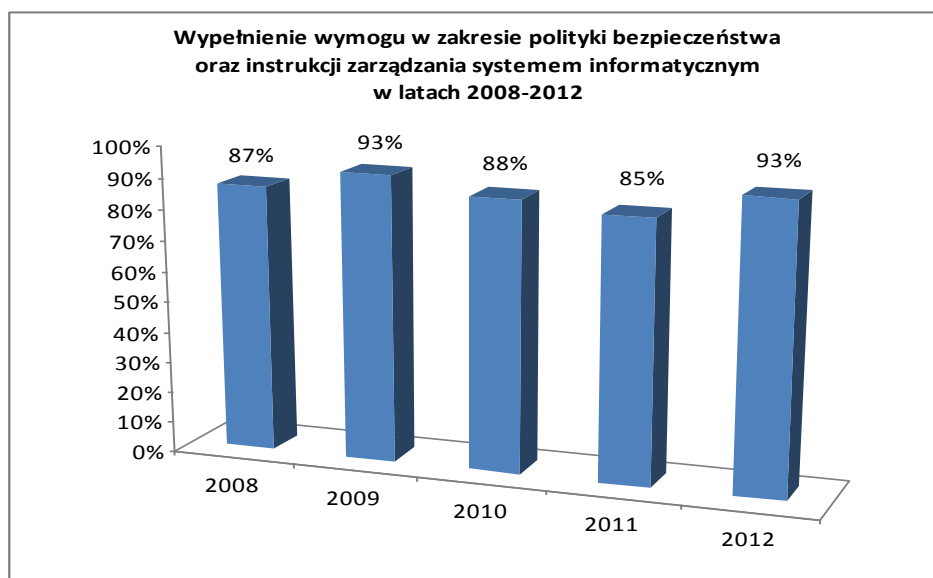
Tylko dwie z ogólnej liczby 165 przeprowadzonych kontroli należały do kategorii kontroli kompleksowych, w których weryfikacją objęto całość problematyki związanej z ochroną danych osobowych. Oznacza to, że kontrolowane były w pełnym zakresie wszystkie przetwarzane przez kontrolowany podmiot zbiory danych oraz wszystkie używane do przetwarzania danych systemy informatyczne.

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

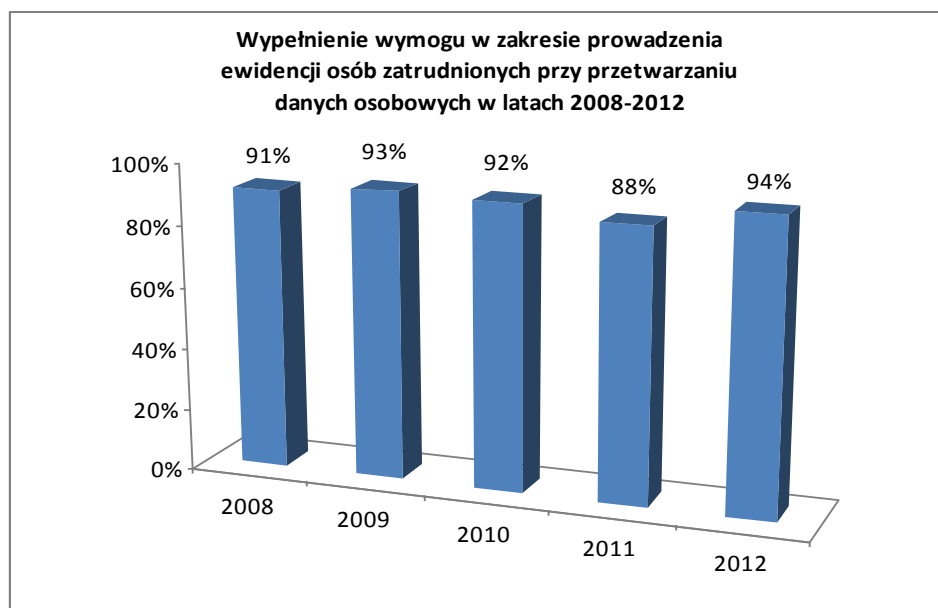
Spełnienie przez kontrolowane podmioty w latach 2007-2012 wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie o ochronie danych osobowych i rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zobrazowana 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 2008-2012 przedstawiono na poniższych wykresach.

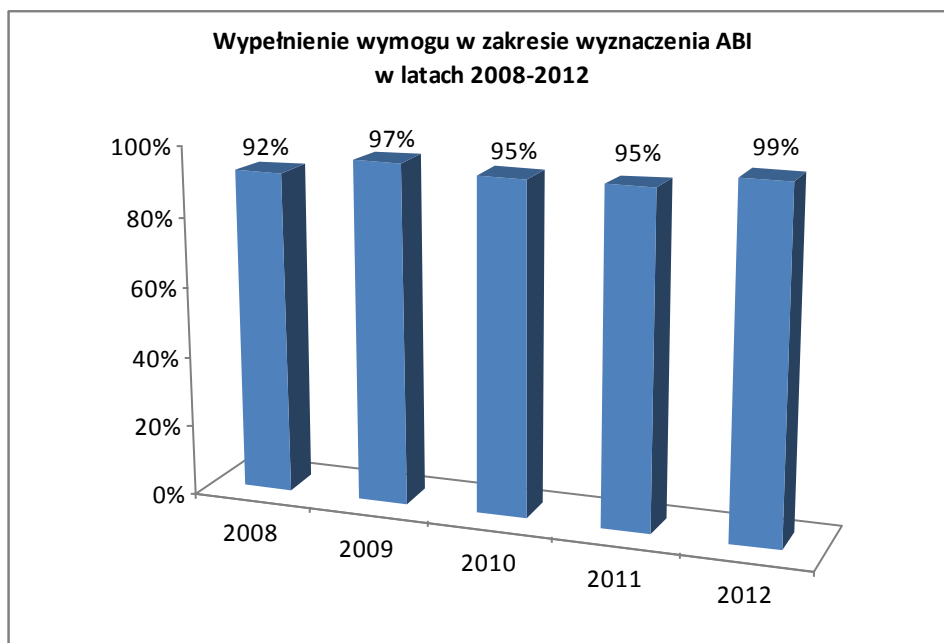


**Wykres 2: *Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych (polityka bezpieczeństwa i instrukcja zarządzania systemem).***



**Wykres 3: *Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.***

Zbiorcze zestawienie wypełnienia wymogów formalnych i organizacyjnych w latach 2008-2012 w zakresie realizacji obowiązku wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji, przedstawiono na poniższym wykresie.



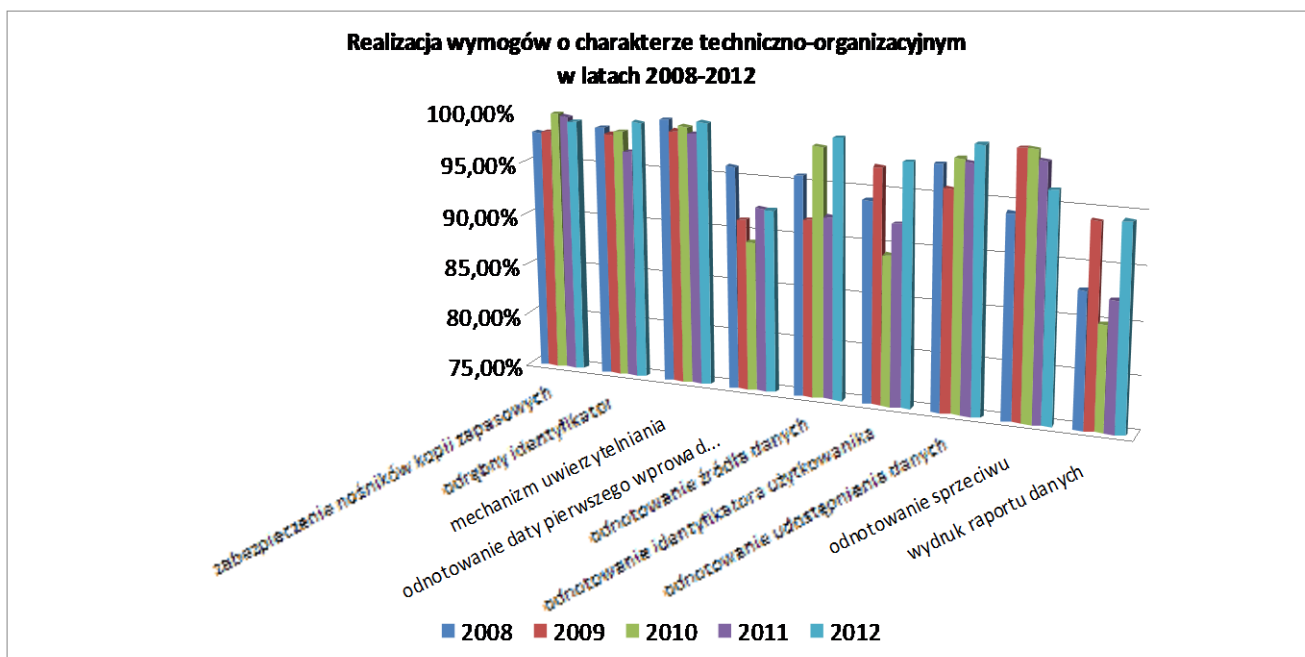
Wykres 4: *Stopień realizacji obowiązku w zakresie wyznaczenia Administratora Bezpieczeństwa Informacji.*

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

Jak już wspomniano, podczas wykonywania czynności kontrolnych w 2012 r. skontrolowano 280 systemów informatycznych służących 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 2012 r. w porównaniu do lat poprzednich, przedstawia Wykres 5.

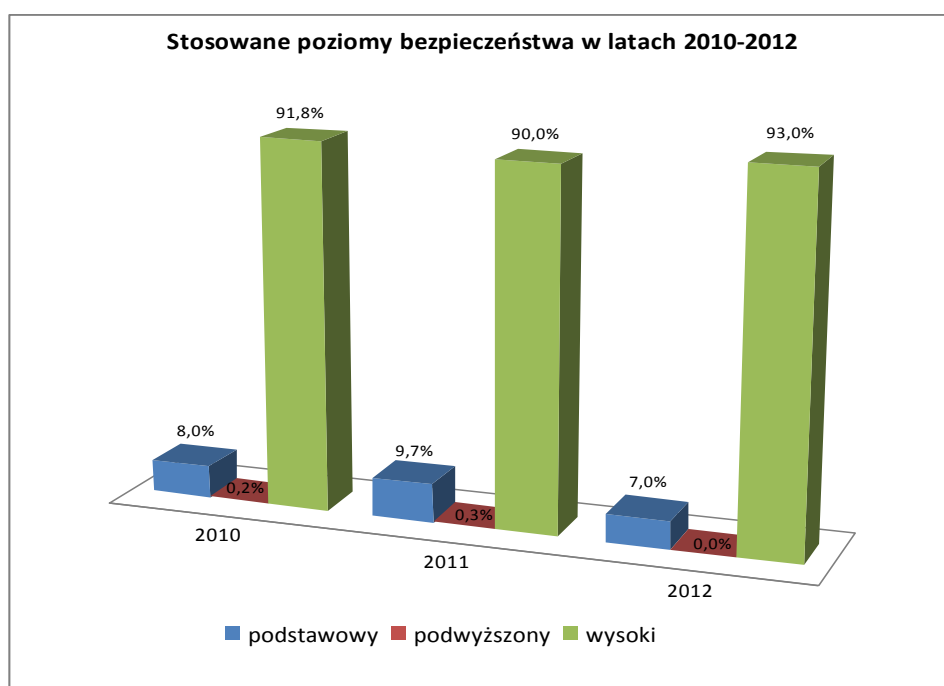




Wykres 5: *Stopień realizacji wymogów technicznych i organizacyjnych w latach 2008-2012.*

Przeprowadzone w 2012 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 2010 - 2012 r. systemów informatycznych przedstawiony został na poniższym wykresie.

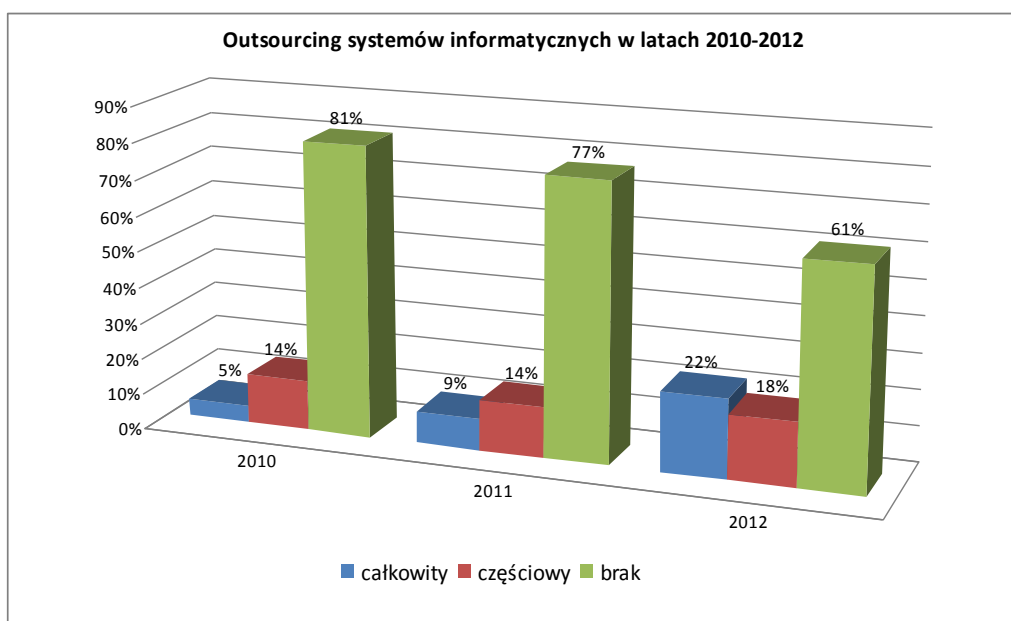


Wykres 6: *Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w latach 2010-2012.*

Jak wynika z ww. wykresu, znaczna część podmiotów skontrolowanych w 2012 r. (tj. 93%) zastosowała wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Stwierdzono również niewielki spadek zabezpieczeń na poziomie podstawowym. Wiąże się to z tym, że część kontrolowanych systemów informatycznych były to systemy, które w większości przypadków były podłączone do sieci publicznej, a co za tym idzie, wystarczającym zabezpieczeniem dla przetwarzanych za pomocą tych systemów danych był poziom podstawowy.

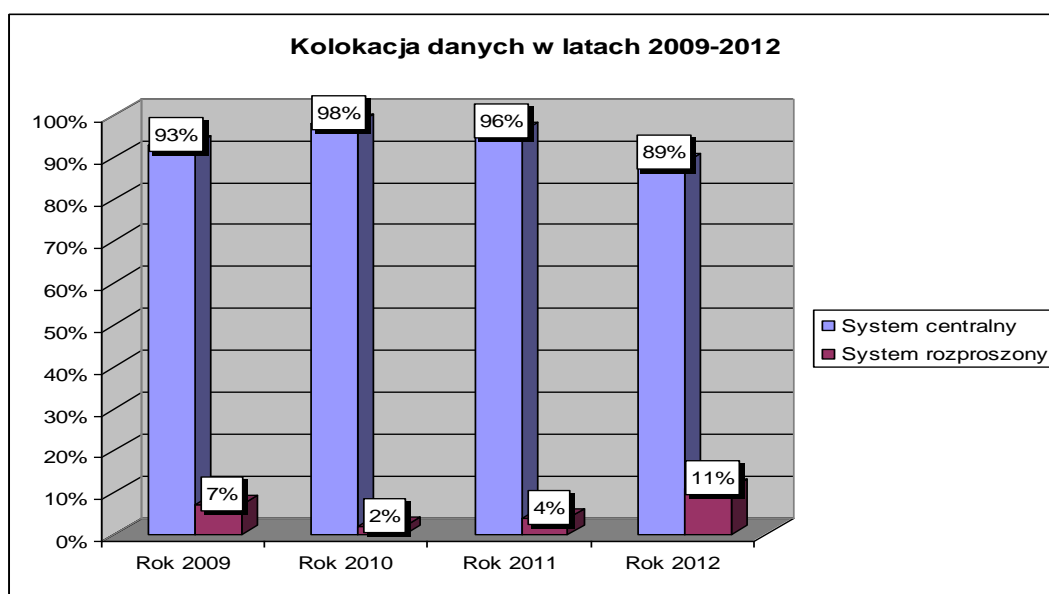
Jak wynika z przeprowadzonych kontroli, większość podmiotów do przetwarzania danych wykorzystywała systemy, nad którymi posiadała w pełni wyłączną kontrolę. Całkowity outsourcing, gdzie proces przetwarzania danych osobowych, jak również oprogramowanie i sprzęt teleinformatyczny administrator danych powierzył w całości do administrowania podmiotom zewnętrznym, w 2012 r. stosowany był w odniesieniu do około 22 % systemów informatycznych. Jest to liczba większa niż w latach ubiegłych. W 2012 r. zauważono natomiast wśród skontrolowanych systemów informatycznych zmniejszenie liczby tych systemów, których obsługą techniczną i administracją zajmowali się pracownicy administratora danych (61 % systemów informatycznych). Niewielkie zmiany w porównaniu do roku 2011 można zaobserwować odnośnie liczby 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 18 % skontrolowanych w 2012 roku systemach.

Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2010-2012 przedstawiono na poniższym wykresie.



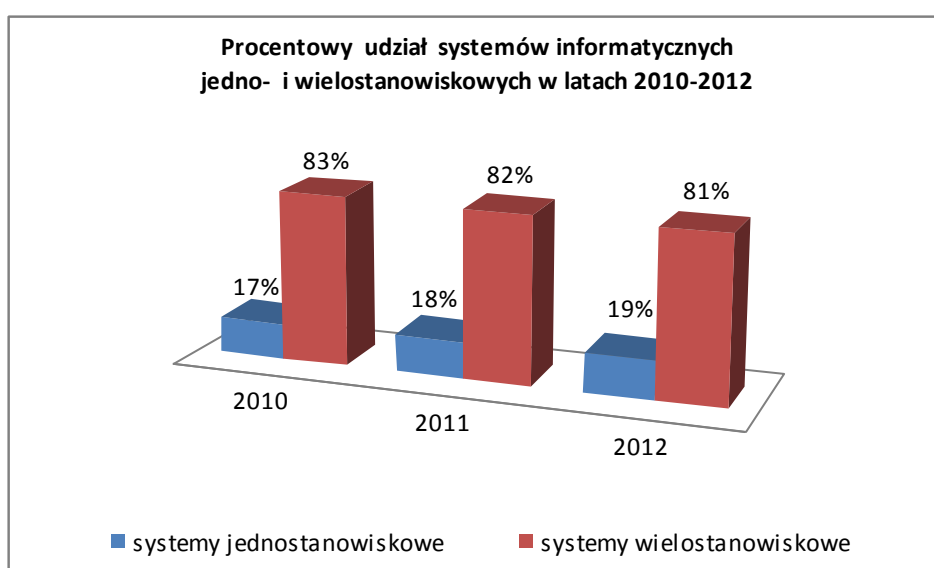
Wykres 7: *Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2010-2012.*

Jak wykazała analiza przetwarzania danych osobowych pod kątem fizycznej lokalizacji danych, u większości skontrolowanych podmiotów dane osobowe zapisywane były w jednym, centralnym miejscu, np. na serwerach znajdujących się w jednym budynku, zazwyczaj w siedzibie kontrolowanego podmiotu. Zauważyć jednak należy, że coraz więcej podmiotów (np. firmy telekomunikacyjne, banki) stosowało zabezpieczenia odnoszące się do ciągłości przetwarzania i bezpieczeństwa danych poprzez stosowanie zapasowych centrów przetwarzania zlokalizowanych w odrębnej lokalizacji. Na poniższym wykresie przedstawiono diagram ilustrujący stopień zastosowania przez kontrolowane podmioty rozwiązań technicznych opartych o systemy centralne i rozproszone.



Wykres 8: *Ilościowy udział centralnego przetwarzania danych w systemach informatycznych objętych kontrolą w latach 2009 - 2012.*

Jak przedstawiono na poniższym Wykresie 9, w 2012 r. w porównaniu z latami 2010-2011 liczba wykorzystywanych wielostanowiskowych systemów informatycznych znajdowała się na zbliżonym 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 wymagała tego specyfika ich stosowania (np. systemy monitoringu).



Wykres 9: *Procentowy udział systemów informatycznych jedno- i wielostanowiskowych wśród systemów objętych kontrolą w latach 2010-2012.*

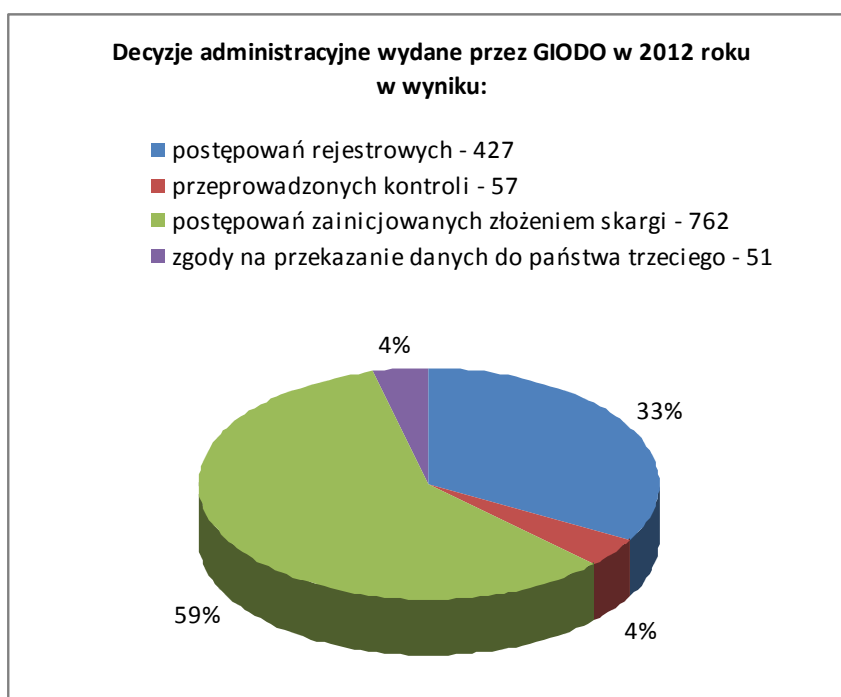
### **3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych**

#### **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. W przypadku stwierdzenia naruszenia przepisów prawa, 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 2012 r. Generalny Inspektor wydał **1297 decyzji administracyjnych**, tj. o 185 więcej w stosunku do roku 2011, w którym wydanych było 1112 decyzji. Spośród 1297 decyzji wydanych w 2012 r. **427 dotyczyło postępowań rejestrowych, 57 zostało wydanych w związku z przeprowadzonymi kontrolami, 762 wydano na skutek postępowania zainicjowanego skargą, zaś 51 dotyczyło zgody na przekazanie danych do państwa trzeciego.** Pośród 1297 decyzji 99 z nich dotyczyło egzekucji administracyjnej. Charakterystyczny jest znaczny wzrost liczby decyzji w postępowaniu zainicjowanym skargą (539 decyzji w 2011 r. i 766 decyzji w 2012). Sytuacja ta związana była przede wszystkim ze zwiększeniem liczby samych skarg oraz z faktem, że skarżący częściej wskazywali na rzeczywiście istniejące problemy dotyczące przetwarzania danych i w precyzyjniejszy sposób zwracali uwagę GODO na zdarzenia, wobec których Generalny Inspektor powinien podjąć działania przewidziane przez Kodeks postępowania administracyjnego i przez ustawę.



*Wykres 10: Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2012 r.*

### **3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa**

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych skierował do organu powołanego do ścigania przestępstw **12 zawiadomień o podejrzeniu popełnienia**

**przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych**, tj. o dwa więcej niż w poprzednim roku sprawozdawczym, w którym wystosowano ich 10.

Wszystkie zawiadomienia złożone zostały w związku z informacjami przekazanymi Generalnemu Inspektorowi Ochrony Danych Osobowych przez podmioty indywidualne. Należy w tym miejscu zaznaczyć, że na ogólną liczbę 12 zawiadomień skierowanych do organów ścigania 7 z nich dotyczyło podejrzenia popełnienia przestępstwa z użyciem Internetu<sup>65</sup>.

W 6 przypadkach zawiadomienie dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w art. 49 ust. 1 ustawy, przetwarzania danych osobowych przez podmioty nieuprawnione<sup>66</sup>. W tym 3 przypadki dotyczyły podejrzenia popełnienia przestępstwa z użyciem Internetu. W jednym z nich administratorzy kilku portali internetowych - w celu umieszczenia ogłoszeń towarzyskich - bezprawnie zamieścili i udostępniali innym osobom na swej stronie internetowej, dane osobowe skarżącej w zakresie jej imienia, nazwiska i daty urodzenia. Nazwy tychże portali jednoznacznie wskazywały na pornograficzny charakter przedmiotowych stron internetowych. Ponadto strona skarżąca wskazała, że prawdopodobnie ten sam podmiot założył jej fikcyjne konto na jednym z portali społecznościowych<sup>67</sup>. Kolejny z przypadków naruszenia art. 49 ust. 1 ustawy dotyczył przetwarzania danych osobowych skarżącej przez spółkę zajmującą się handlem wysyłkowym, pomimo wniesienia uprzedniego sprzeciwu. Jednocześnie spółka nie była w stanie udowodnić, w jaki sposób i od jakiego podmiotu pozyskała dane osobowe skarżącej<sup>68</sup>. W pozostałych przypadkach przedmiotem zawiadomień uczyniono podejrzenie popełnienia przestępstwa przez podmioty prowadzące strony internetowe poprzez przetwarzanie danych osobowych bez podstawy prawnej<sup>69</sup>.

Ponadto w 5 przypadkach zawiadomienia dotyczyły przestępstwa wskazanego w art. 51 ustawy, tj. udostępnienia danych osobowych podmiotom nieupoważnionym. Jedna z takich spraw opisywała przypadek zawarcia przez spółdzielnię mieszkaniową umowy z apteką, w wyniku której nastąpiło przekazanie danych osobowych członków spółdzielni w celu wykonania imiennych kart rabatowych<sup>70</sup>. Inne z zawiadomień dotyczyło opublikowania danych osobowych w zakresie imienia, nazwiska, nazwy firmy, adresu i numeru telefonu na stronach internetowych oraz ich przekazania spółce, pomimo wyraźnego sprzeciwu osób, których dane dotyczą<sup>71</sup>. Kolejne zawiadomienie dotyczyło podmiotu zajmującego się usługami medycznymi, który wskutek eksmisji opuszczając należący do niego lokal

---

<sup>65</sup> DOLiS/ZAW-4/12/27621, DOLiS/ZAW-5/12/30166, DOLiS/ZAW-7/12/42561, DOLiS/ZAW-8/12/43284, DOLiS/ZAW-9/12/52367, DOLiS/ZAW-10/12/52376, DOLiS/ZAW-11/12/55012.

<sup>66</sup> DOLiS/ZAW-1/12/1889, DOLiS/ZAW-5/12/30166, DOLiS/ZAW-6/12/36235, DOLiS/ZAW-9/12/52367, DOLiS/ZAW-11/12/55012, DIS/ZAW-2/12/10355.

<sup>67</sup> DOLiS/ZAW-11/12/55012

<sup>68</sup> DOLiS/ZAW-6/12/36235

<sup>69</sup> DOLiS/ZAW-5/12/30166, DOLiS/ZAW-9/12/52367.

<sup>70</sup> DOLiS/ZAW-3/12/10373

<sup>71</sup> DOLiS/ZAW-10/12/52376

użytkowy, pozostawił w nim karty pacjentów, recepty oraz inną dokumentację medyczną bez należytego zabezpieczenia<sup>72</sup>. W pozostałych przypadkach przedmiotem zawiadomień uczyniono podejrzenie popełnienia przestępstwa poprzez przesłanie wiadomości e-mail do kilkuset adresatów w ten sposób, że dla każdego z nich widoczne były adresy poczty elektronicznej pozostałych, albo zawierającej w swojej treści dane osobowe klientów spółki<sup>73</sup>.

W jednym z zawiadomień Generalny Inspektor stwierdził wypełnienie znamion czynu zabronionego wskazanego w art. 49 oraz w art. 52 ustawy o ochronie danych osobowych. W przedmiotowej sprawie skarżąca poddała się w poradni szpitala badaniom lekarskim, następnie zatelefonował do niej pracownik spółki z propozycją zawarcia umowy ubezpieczenia na wypadek zachorowania na chorobę, której dotyczyły owe badania. W ocenie Generalnego Inspektora powyższe uzasadniało podejrzenie nieuprawnionego udostępnienia dotyczących jej danych osobowych, w tym ewentualnie danych o jej stanie zdrowia, przez szpital na rzecz spółki<sup>74</sup>.

Natomiast tylko jedno zawiadomienie dotyczyło przestępstw wskazanych zarówno w art. 51 i art. 52 ustawy o ochronie danych osobowych. W omawianym przypadku Generalny Inspektor uzyskał informację, że sklep internetowy udostępnił za pośrednictwem poczty elektronicznej adresy e-mail bardzo dużej liczby osób przy okazji rozsyłania ofert marketingowych<sup>75</sup>.

Spośród wspomnianych 12 zawiadomień skierowanych przez GODO do organów ścigania, tylko jedno miało związek z przeprowadzonymi kontrolami<sup>76</sup>. W 2012 r. w związku ze skargą pracowników spółki dotyczącą wykorzystania ich danych osobowych na potrzeby kampanii wyborczej, Generalny Inspektor skierował do prokuratury rejonowej zawiadomienie o podejrzeniu popełnienia przestępstwa określonego w art. 49 ust. 1 ustawy o ochronie danych osobowych, polegającego na przetwarzaniu danych osobowych bez podstawy prawnej. W wyniku przeprowadzonej w spółce kontroli ustalono, że do pracowników spółki zostały skierowane informacje zachęcające do głosowania na kandydatkę jednego z komitetów wyborczych. Ww. informacje zostały przesłane pocztą w postaci imiennie zaadresowanych przesyłek. W tym celu wykorzystane zostały dane osobowe w zakresie imion, nazwisk i adresów osób, będących odbiorcami ww. przesyłek. W toku kontroli przeprowadzonej w spółce nie potwierdzono faktu udostępnienia przez kontrolowany podmiot danych osobowych pracowników na potrzeby kampanii wyborczej. Jednocześnie ustalono, że osoby, które otrzymały ww. informacje wyborcze nie udostępniały swoich danych osobowych na potrzeby prowadzenia kampanii wyborczej. Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych zwrócił się do komitetu wyborczego z pytaniem o źródło, z którego pozyskał dane osobowe pracowników spółki. Komitet

---

<sup>72</sup> DOLiS/ZAW-12/12/72614

<sup>73</sup> DOLiS/ZAW-4/12/27621, DOLiS/ZAW-8/12/43284.

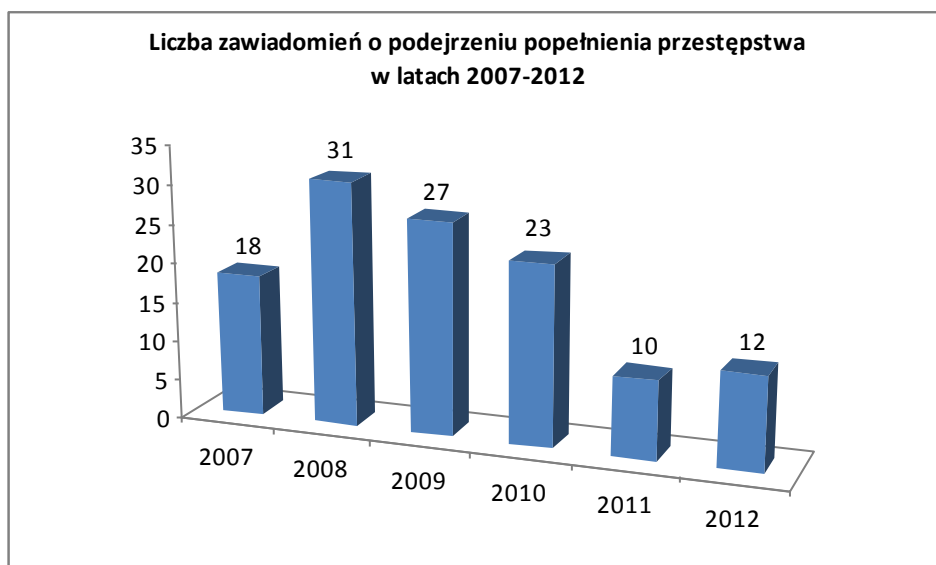
<sup>74</sup> DOLiS/ZAW-1/12/1889

<sup>75</sup> DOLiS/ZAW-7/12/42561

<sup>76</sup> DIS/ZAW-2/12/10355 dot. DIS-K-421/109/11.

wyborczy nie udzielił odpowiedzi na ww. pytanie, jednocześnie informując, iż nie wyrażał zgody na prowadzenie agitacji wyborczej z wykorzystaniem danych osobowych pracowników spółki. Komitet wskazał, iż zgodnie z art. 67 ustawy z dnia 16 lipca 1998 r. Ordynacja wyborcza do rad gmin, rad powiatów i sejmików województw (Dz. U. z 1998 r. Nr 95, poz. 602 z późn. zm.), zakazana jest każda forma agitacji wyborczej bez uprzedniej zgody pełnomocnika wyborczego komitetu wyborczego. W związku z powyższym, jakiegokolwiek działania o charakterze agitacji wyborczej związane z pozyskaniem danych osobowych pracowników spółki zostały dokonane bez wiedzy i zgody pełnomocnika wyborczego ww. komitetu. Następnie Generalny Inspektor Ochrony Danych Osobowych skierował identyczne pytanie do kandydatki, do głosowania na którą zachęcały informacje wyborcze przesłane pracownikom spółki. Na ww. pytanie nie uzyskał odpowiedzi. Z uwagi na to, iż pracownicy spółki nie wyrażali zgody na przetwarzanie swoich danych osobowych na potrzeby kampanii wyborczej, jak również ze względu na niemożliwość ustalenia, czy ww. dane osobowe przetwarzane były na podstawie innych przesłanek legalizujących przetwarzanie danych, zachodziło uzasadnione podejrzenie, iż ich przetwarzanie odbywało się z naruszeniem przepisów prawa.

Liczbę zawiadomień o podejrzeniu popełnienia przestępstwa składanych przez Generalnego Inspektora w latach 2007-2012 przedstawia Wykres 11.

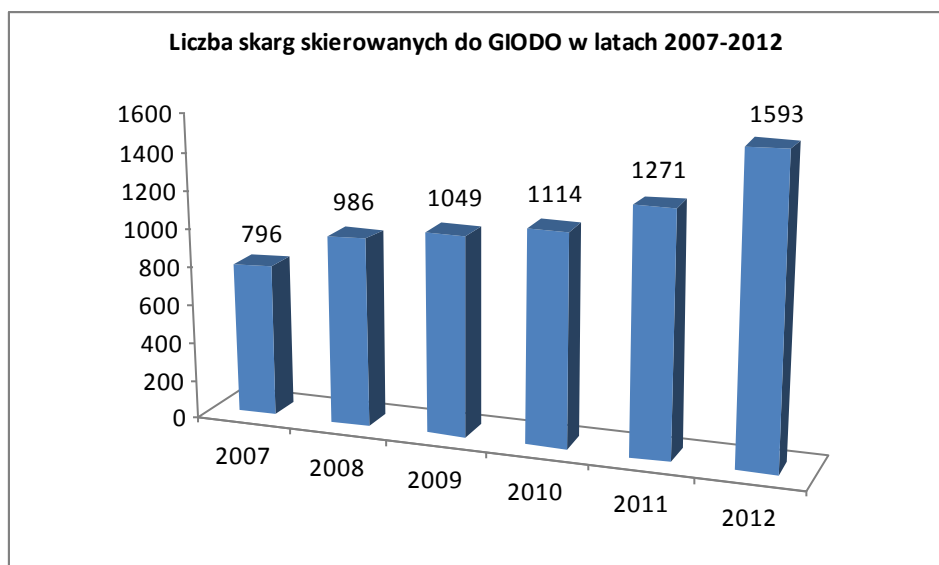


**Wykres 11: Porównanie liczby zawiadomień o podejrzeniu popełnienia przestępstwa skierowanych przez GIODO do organów ścigania w latach 2007–2012.**



### 3.3. Rozpatrywanie skarg

W 2012 r. do Departamentu Orzecznictwa, Legislacji i Skarg Biura GODO wpłynęły **1593 skargi** dotyczące naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2011, w którym wpłynęło 1271 skarg, liczba ta uległa zwiększeniu o 322, co przedstawia Wykres 12.

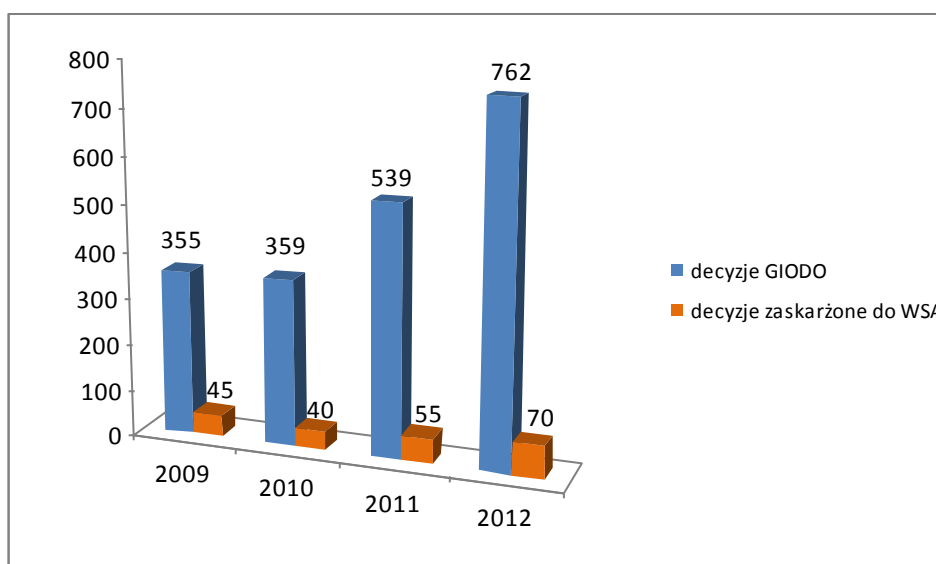


*Wykres 12: Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007–2012 r.*

Każda ze skarg analizowana była na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego i ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz. U. Nr 225, poz. 1635 z późn. zm.). W sytuacji, gdy skarga nie spełniała warunków wymaganych przez ww. przepisy prawa, organ ochrony danych osobowych wzywał wnioskodawcę do uzupełnienia braków formalnych. Wskutek braku reakcji wiele skarg z 2012 roku zostało pozostawionych bez rozpoznania, bądź też zwróconych do wnioskodawców. W przypadku tych, które je spełniały, Generalny Inspektor Ochrony Danych Osobowych wszczynał 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 sytuacji, gdy Generalny Inspektor nie stwierdzał naruszenia prawa, wydawał decyzje administracyjne odmawiające uwzględnienia wniosku.

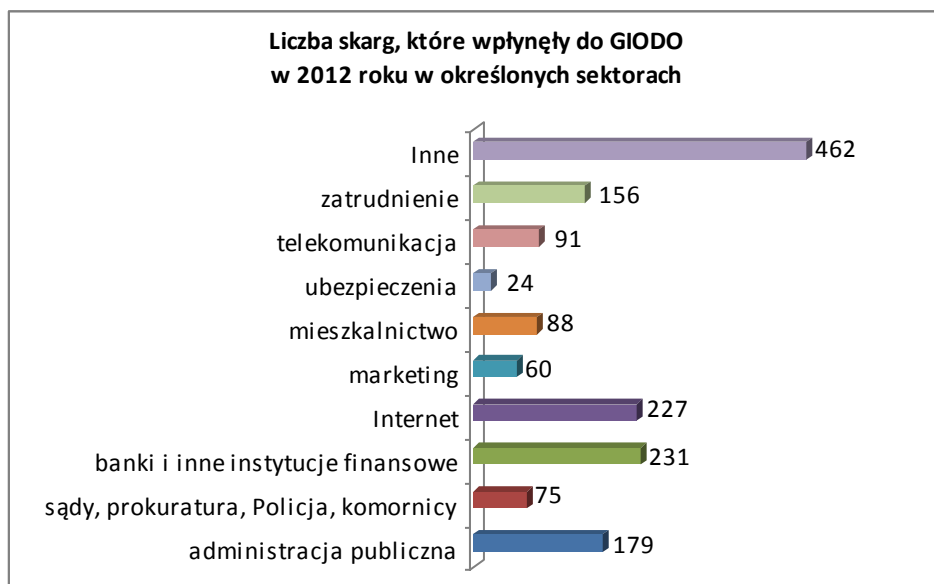
W postępowaniach zainicjowanych skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, wydane zostały **762 decyzje administracyjne, czyli o 223 więcej niż w roku 2011, w którym wydano ich 539**. Oznacza to wzrost liczby decyzji wydanych w 2012 r. o ponad 41 %. Sytuacja ta związana jest przede wszystkim ze zwiększeniem liczby skarg, w których skarżący coraz precyzyjniej artykułowali swoje oczekiwania wobec organu ds. ochrony danych osobowych w kwestii podjęcia działań przewidzianych przez Kodeks postępowania administracyjnego i ustawę o ochronie danych osobowych.

Spośród 462 decyzji administracyjnych wydanych w 2012 r. na skutek postępowań zainicjowanych złożeniem skargi, 70 z nich zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie (WSA). W porównaniu z rokiem 2011, w którym 55 decyzji zostało zaskarżonych, oznacza to wzrost o 15 spraw.



**Wykres 13: Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2012 w związku z rozpatrywanymi skargami.**

Analizując treść skarg można wyróżnić 10 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) telekomunikacja, 9) zatrudnienie i 10) inne.

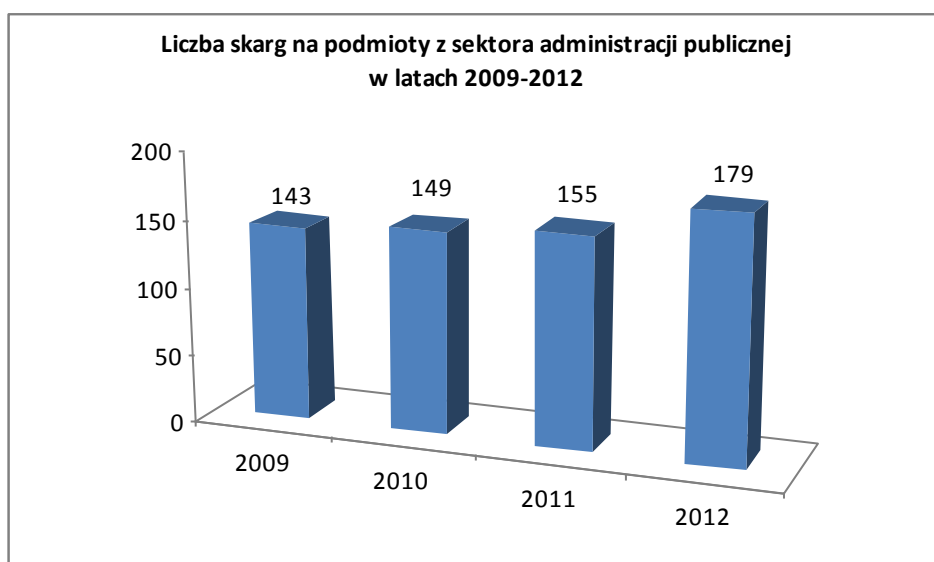


*Wykres 14: Zestawienie porównawcze liczby skarg, które wpłynęły do Biura GIODO w 2012 r. w określonych sektorach.*

Poniżej zostaną przedstawione przykłady skarg, które wpłynęły w 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych na podmioty działające w wybranych obszarach.

#### **1) Administracja publiczna**

W omawianym roku 2012, do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **179** skarg dotyczących sektora **administracji publicznej**, tj o 24 więcej niż w 2011 r.



*Wykres 15: Zestawienie porównawcze liczby skarg na podmioty z sektora administracji publicznej, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2012.*

W omawianym okresie GODO wydał decyzję nakazującą burmistrzowi udostępnienie skarżącemu danych osobowych w zakresie imion i nazwisk osób, które wniosły na niego do urzędu miasta skargę w przedmiocie zasad współżycia społecznego<sup>77</sup>. Przed zwróceniem się do GODO skarżący wystąpił do burmistrza o udostępnienie mu ww. danych tych osób, w celu prawidłowego wytoczenia przeciwko nim prywatnego aktu oskarżenia o pomówienie, tj. o czyn z art. 212 § 2 Kodeksu karnego. W ocenie Generalnego Inspektora wykorzystanie danych w celu realizacji konstytucyjnie przysługującego prawa 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 pozbawić go możliwości obrony jego praw i prowadzić do nieuzasadnionej ochrony pomawiających go osób przed ewentualną odpowiedzialnością za swoje działania. Zwłaszcza, że osoby te mogły w trakcie postępowania sądowego w pełni korzystać z praw zagwarantowanych przepisami ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz. 555 z późn. zm.). Działanie burmistrza polegające na nieudostępnieniu skarżącemu danych osobowych, mogło także doprowadzić do ograniczenia zagwarantowanego konstytucyjnie prawa skarżącego do sądu oraz skutecznie ochronić sprawcę przed odpowiedzialnością za popełniony czyn.

W 2012 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło pismo, w którym wskazano, że skarżący znalazł na chodniku przed swoją posesją, foliową przezroczystą koszulkę zawierającą plik dokumentów zapakowanych w kopertę, opatrzoną danymi osobowymi jego i jego żony w zakresie imion, nazwisk oraz adresu zamieszkania<sup>78</sup>. Dokumenty te dotyczyły likwidacji szkoły, do której uczęszczają jego dzieci. Wójt potwierdził powyższe wyjaśniając jednocześnie, że z uwagi na fakt, iż rodzice dzieci likwidowanej szkoły, a także dorośli domownicy, uchylali się od odbierania powiadomień, był on zmuszony do zastosowania innego trybu, tj. pozostawiania dokumentów w bramach posesji. Wobec powyższego Generalny Inspektor wystąpił do urzędu gminy w celu zasygnalizowania, iż w przedmiotowej sprawie niewątpliwie doszło do uchybień w procesie przetwarzania danych osobowych skarżących, poprzez ich niewłaściwe zabezpieczenie przed dostępem osób nieupoważnionych<sup>79</sup>. Zgromadzony w sprawie materiał dowodowy jednoznacznie potwierdził, iż koperta z dokumentami zawierającymi dane osobowe skarżących została umieszczona przez pracowników urzędu gminy na bramie ich posesji, przed którą *notabene* znajdował się przystanek autobusowy. W ocenie organu takie rozporządzanie danymi osobowymi mogło skutkować zapoznaniem się z ich treścią przez nieograniczoną liczbę osób do tego nieupoważnionych.

---

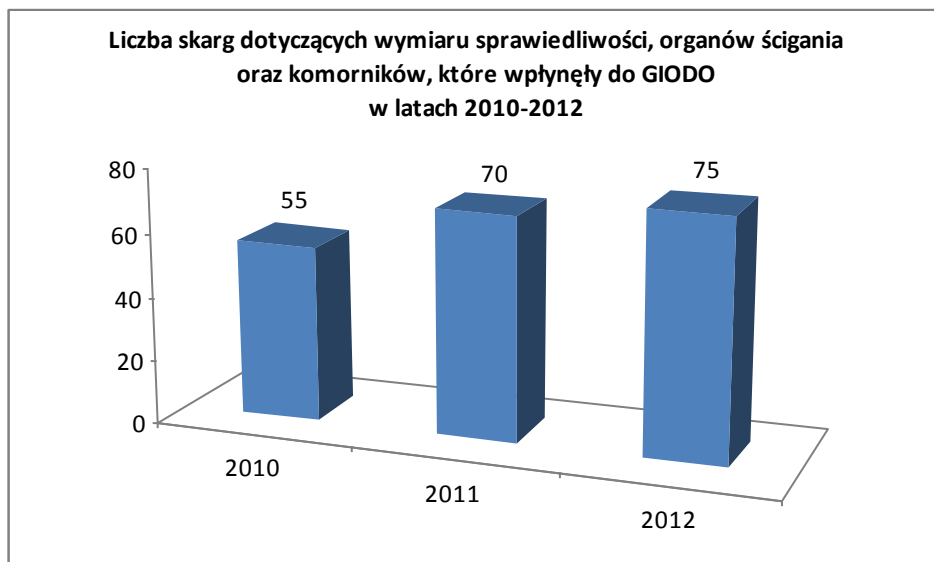
<sup>77</sup> Decyzja GODO z dnia 17 maja 2012 r. znak: DOLiS/DEC-436/12/30724, 30728.

<sup>78</sup> DOLiS-440-297/12

<sup>79</sup> Pismo GODO z dnia 2 sierpnia 2012 r. znak: DOLiS-440-297/12/47541.

## 2) Sądy, prokuratura, policja, komornicy

W analizowanym okresie do GODO wpłynęło **75** skarg dotyczących sektora **sądów, prokuratury, policji i komorników**. Stanowi to nieznaczny wzrost w stosunku do roku 2011, w którym wpłynęło 70 skarg na podmioty działające w tym sektorze.



Wykres 16: *Zestawienie porównawcze liczby skarg dotyczących sektora sądów, prokuratury, policji i komorników, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2012.*

W 2012 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga na udostępnienie danych osobowych przez starostę na rzecz komornika. Dłużniczka nie wywiązywała się ze świadczeń na rzecz starosty z tytułu użytkowania wieczystego nieruchomości. Starosta uzyskał tytuły wykonawcze zaopatrzone w klauzule wykonalności, w celu wyegzekwowania zaległych należności. Jednak postępowanie egzekucyjne wobec dłużniczki okazało się bezskuteczne. Wobec powyższego komornik wezwał starostę do uzupełnienia wniosku o wszczęcie egzekucji poprzez wskazanie wierzytelności i innych praw majątkowych dłużniczki, jej miejsca pracy oraz kont bankowych i ich numerów. W odpowiedzi na wezwanie starosta przekazał komornikowi pismo zawierające oświadczenie dłużniczki o dochodach i dwie umowy najmu, w tym umowę najmu pomiędzy dłużniczką a skarżącym, zawierającą jego dane osobowe, z których to dochodów komornik mógł przeprowadzić skuteczną egzekucję. W przedstawionej sprawie Generalny Inspektor wydał decyzję odmawiającą uwzględnienia wniosku skarżącego, ponieważ udostępnienie danych osobowych miało swoje prawne uzasadnienie w przepisie art. 797 Kodeksu postępowania cywilnego (K.p.c.) w zw.

z art. 23 ust 1 pkt 2 ustawy o ochronie danych osobowych<sup>80</sup>. W myśl art. 797 §1 K.p.c. we wniosku lub żądaniu przeprowadzenia egzekucji z urzędu należy wskazać świadczenie, które ma być spełnione, oraz sposób egzekucji. Do wniosku lub żądania należy dołączyć tytuł wykonawczy. Jak podkreśla się w doktrynie, z cytowanego przepisu bezsprzecznie wynika, że „(...) określając sposób egzekucji świadczeń pieniężnych wierzyciel wskazuje, z jakich składników majątku dłużnika ma być prowadzona egzekucja. W doktrynie i judykaturze nie pozostawia się wątpliwości, że składniki te powinny być przez wierzyciela dokładnie oznaczone (...) Przy egzekucji z wierzytelności niedopuszczalne jest żądanie przeprowadzenia egzekucji z wszelkich wierzytelności dłużnika – należy oznaczyć tytuł prawny oraz podmiot, względem którego istnieje dług. (...) Jedynie w przypadku egzekucji z ruchomości wystarczy, że wierzyciel zażąda przeprowadzenia egzekucji ze wszystkich ruchomości znajdujących się we władaniu dłużnika”<sup>81</sup>.

W kolejnej sprawie Generalny Inspektor Ochrony Danych Osobowych wystąpił do komendy policji z pismem sygnalizującym nieprawidłowości w przetwarzaniu danych osobowych<sup>82</sup>. Z ustaleń dokonanych przez Generalnego Inspektora wynikało, że osoba, której danych dotyczyło postępowanie, została zatrzymana przez policjantów pełniących służbę w komendzie. W sprawie tej przeprowadzono czynności wyjaśniające w trybie przepisów ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2008 r. Nr 133, poz. 848 z późn. zm.) i m.in. sprawdzono, że osoba zatrzymana złożyła w Rzeczypospolitej Polskiej wniosek o nadanie jej statusu uchodźcy. Następnie przesłany został do innej komendy policji telegram zawierający informację o dokonanym zatrzymaniu, w którym, wśród danych identyfikujących osobę zatrzymaną, została zawarta informacja o miejscu jej pobytu na terenie Rzeczypospolitej Polskiej - Ośrodek dla Uchodźców. Telegram ten, po zaakceptowaniu przez zastępcę dyżurnego komendy policji, został przesłany do Ambasady Republiki Białoruś. Komendant policji w złożonych w sprawie wyjaśnieniach poinformował, że obowiązek powiadomienia o zatrzymaniu osoby wnoszącej skargę wynikał z dyspozycji art. 38 ust. 2 Konwencji Konsularnej między Rzeczpospolitą Polską a Republiką Białoruś, sporządzonej w Warszawie dnia 2 marca 1992 r. (Dz. U. z 1994 r. Nr 50, poz. 197).

W ocenie Generalnego Inspektora niedopuszczalne było przekazanie przez komendanta policji informacji o miejscu pobytu skarżącego na rzecz Ambasady Republiki Białoruś. Art. 9 ustawy z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2012, poz. 680) przewiduje, że dane cudzoziemca, na podstawie których jest możliwe ustalenie, że: (pkt 1) postępowanie o nadanie statusu uchodźcy, udzielenie azylu lub zgody na pobyt tolerowany wobec cudzoziemca jest w toku lub zakończyło się, (pkt 2) cudzoziemcowi nadano lub odmówiono

<sup>80</sup> DOLiS/DEC-749/12 dot. DOLiS-440-471/12.

<sup>81</sup> Komentarz do ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego. Jakubecki A.(red.), Bodio J., Demendecki T., Marcewicz O., Telenga P., Wójcik M.P. LEX/el., 2011.

<sup>82</sup> Pismo GIODO z dnia 23 listopada 2012 r. znak: DOLiS-440-1062/11/71430/12.

nadania statusu uchodźcy, (pkt 3) cudzoziemcowi udzielono lub odmówiono udzielenia azylu lub zgody na pobyt tolerowany, (pkt 4) cudzoziemcowi udzielono lub odmówiono udzielenia ochrony uzupełniającej - nie mogą być udostępniane władzom oraz instytucjom publicznym kraju jego pochodzenia. Zdaniem Generalnego Inspektora przekazana Ambasadzie Republiki Białoruś informacja, iż miejscem pobytu skarżącego na terenie Rzeczypospolitej Polskiej jest „Ośrodek dla Uchodźców” jest informacją umożliwiającą ustalenie, że toczy lub toczyło się postępowanie o nadanie statusu uchodźcy, bowiem zakwaterowanie w ośrodku to jedna z form pomocy dla cudzoziemców ubiegających się o nadanie statusu uchodźcy, przewidzianych w rozdziale 5 działu II ustawy o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej. Zatem przekazanie tej informacji ambasadzie kraju pochodzenia skarżącego naruszyło zakaz wskazany w art. 9 przywołanej ustawy. Odnosząc się do wyjaśnień komendanta policji Generalny Inspektor wskazał, że realizując obowiązek wynikający z umowy międzynarodowej administrator danych musi mieć na uwadze to, czy ze względu na treść konkretnej informacji (w niniejszej sprawie – informacji o miejscu pobytu skarżącego) jej udostępnienie w związku z realizacją tego obowiązku nie naruszy przepisów innych aktów prawnych. Zgodnie bowiem z art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem.

W omawianym roku sprawozdawczym do Biura Generalnego Inspektora wpłynęła skarga byłego funkcjonariusza policji, którego dane osobowe zostały wykorzystane w celach prywatnych w związku z wniesieniem do sądu przez komendanta policji i jego zastępcę, roszczenia prywatno-skargowego w sprawie o naruszenie dóbr osobistych. Dane osobowe skarżącego, które wykorzystano w postępowaniu cywilnym, zawarte były w sprawozdaniu z czynności wyjaśniających przeprowadzonych przez komendę policji, w której pracował. Sprawozdanie zostało załączone do pozwu w sprawie cywilnej jako „materiał poglądowy”. W związku z powyższym Generalny Inspektor wystąpił do komendanta policji o wprowadzenie odpowiednich środków organizacyjnych wobec podległych mu funkcjonariuszy, mających na celu wzmocnienie ochrony danych osobowych, celem uniknięcia podobnych uchybień w przyszłości<sup>83</sup>. Organ zwrócił uwagę, że przetwarzanie danych osobowych winno odbywać się zgodnie z zasadami określonymi w przepisach ustawy o ochronie danych osobowych. Oznacza to, że funkcjonariusze policji muszą legitymować się przesłanką przetwarzania danych wskazaną w art. 23 ust. 1 pkt 1- 5 lub art. 27 ust. 2 pkt 1- 10 ustawy o ochronie danych osobowych, jak również zasadami wynikającymi z jej art. 26. Funkcjonariusze komendy, którzy wykorzystali przedmiotowe sprawozdanie jako dowód w postępowaniu prywatno-skargowym

---

<sup>83</sup> Pismo GIODO z dnia 31 grudnia 2012 r. znak: DOLiS-440-156/12/78393.

dotyczącym naruszenia ich dóbr osobistych, zobowiązani byli w pierwszej kolejności zwrócić się do administratora danych osobowych zawartych w treści tego dokumentu z wnioskiem w zakresie zmiany celu, w jakim dane te były przetwarzane. Decyzja w tym zakresie należy do administratora danych osobowych, który musi każdorazowo rozważyć, czy istnieją podstawy dla takiego działania.

Na uwagę zasługuje również przykład skargi na jedną z komend policji, która stworzyła możliwość pozyskania przez osoby nieupoważnione danych osobowych swojego pracownika, wobec którego toczyło się postępowanie dyscyplinarne. Z wyjaśnień uzyskanych w toku prowadzonego postępowania wynikało, że komenda, chcąc doręczyć korespondencję lekarzowi medycyny w związku toczącym się postępowaniem dyscyplinarnym wobec jego pacjenta, nie miała możliwości doręczenia jej osobiście. W chwili gdy jej funkcjonariusz dotarł pod adres wskazany na pieczęcie lekarskiej widniejącej na dokumencie wystawionym przez lekarza, gabinet lekarski był już zamknięty. W związku z faktem, że pod tym samym adresem znajdował się także zakład fryzjerski oraz że numer telefonu kontaktowego do gabinetu lekarza był jednocześnie numerem do zakładu fryzjerskiego - co w ocenie komendy sugerowało współpracę tych podmiotów - funkcjonariusz przekazał korespondencję pracownicy zakładu fryzjerskiego. Komendant podjął przedmiotowe czynności w celu uzyskania informacji od lekarza medycyny, który orzekł czasową niezdolność do pracy pracownika, wobec którego prowadzone było postępowanie dyscyplinarne, na temat możliwości jego uczestnictwa w czynnościach dowodowych oraz zapoznania się z aktami postępowania dyscyplinarnego.

W piśmie skierowanym do komendy Generalny Inspektor wskazał<sup>84</sup>, że w przypadku gdy komendant nie ma możliwości uzyskania przedmiotowej informacji od lekarza orzekającego o niezdolności do pracy, to zgodnie z art. 135f ust. 10 zd. 2 ustawy o Policji powinien zwrócić się do lekarza, który obecnie leczy obwinionego, a w dalszej kolejności do lekarza o takiej samej specjalności, w celu uzyskania od niego ewentualnej zgody. GODO wskazał również na treść § 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 listopada 2008 r. w sprawie szczegółowego trybu wykonywania czynności związanych z postępowaniem dyscyplinarnym w stosunku do policjantów (Dz. U. Nr 198, poz. 1933). W ww. przepisie wskazano, że dokumenty można doręczać bezpośrednio, przekazywać przesyłką listową, pocztą elektroniczną, faksem lub przy użyciu innych środków łączności (ust. 1). Obieg dokumentów prowadzi się w taki sposób, aby ich treść nie była udostępniona osobom niepowołanym (ust. 2). GODO podkreślił, że to komendant, jako podmiot prowadzący postępowanie dyscyplinarne wobec skarżącego, był zobowiązany do przetwarzania jego danych osobowych zgodnie z prawem, w tym do nieudostępnienia przedmiotowych danych osobom nieupoważnionym.

---

<sup>84</sup> Pismo GODO z dnia 14 maja 2012 r. znak: DOLiS-440-46/12/29623.



Wśród wielu skarg na podmioty omawianego sektora znalazły się te dotyczące przetwarzania danych osobowych skarżących w Krajowym Systemie Informacji Policji (KSIP)<sup>85</sup>. W decyzjach wydanych w 2012 roku z tego zakresu, Generalny Inspektor nakazywał komendantowi policji usunięcie danych osobowych skarżących z tego systemu<sup>86</sup>. Wskazywał przy tym, że przy ocenie zasadności odmowy usunięcia danych osobowych ze zbioru KSIP zastosowanie znajduje § 11 ust. 3 rozporządzenia w sprawie przetwarzania przez policję informacji o osobach<sup>87</sup>. Przepis ten przewiduje możliwość usunięcia danych po dokonaniu oceny przetwarzanych informacji o osobach pod kątem ich przydatności w prowadzonych postępowaniach oraz niezbędności w realizacji ustawowych zadań policji. Niemniej jednak, jak podkreślił Generalny Inspektor, powyższa regulacja nie zawiera jednoznacznych zapisów o terminie przechowywania danych. W ocenie organu ochrony danych osobowych, w obecnym stanie prawnym w kwestii przetwarzania danych osobowych w KSIP zastosowanie będą miały przepisy ustawy o ochronie danych osobowych.

GIODO podkreślił, że każdy przypadek przetwarzania w KSIP danych osobowych musi odbywać się z poszanowaniem zasad wyznaczonych przepisami ustawy o ochronie danych osobowych. Zdaniem organu dalsze przetwarzanie w KSIP danych skarżących należało uznać za zbędne dla realizacji celu, jakim była realizacja zadań ustawowych policji oraz możliwość wykorzystania zgromadzonych informacji w innych postępowaniach. Skoro nie były prowadzone jakiejkolwiek czynności przeciwko skarżącym przez policję, działanie powyższe narażało komendanta policji - jako administratora przedmiotowych danych - na zarzut naruszenia wskazanego powyżej art. 26 ust. 1 ustawy o ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych, podobnie jak w poprzednich latach, konsekwentnie stoi na stanowisku, że prawodawca nie określił konkretnych kryteriów pozwalających na dokonanie oceny przydatności danych osobowych znajdujących się w KSIP, lecz posłużył się kryteriami ogólnymi, które wymagają każdorazowo wnikliwej analizy w odniesieniu do konkretnego przypadku.

Jednocześnie należy wskazać, że w 2012 r. występowały sprawy<sup>88</sup> dotyczące przetwarzania danych osobowych w KSIP przez policję, w których dzięki działaniom organu ochrony danych osobowych na etapie prowadzenia postępowania wyjaśniającego, komendant weryfikował zasadność przetwarzania tychże danych. Wskutek powyższych działań dochodziło do usuwania danych osobowych skarżących ze zbiorów KSIP.

---

<sup>85</sup> m.in. DOLiS-440-109/12, DOLiS-440-269/12.

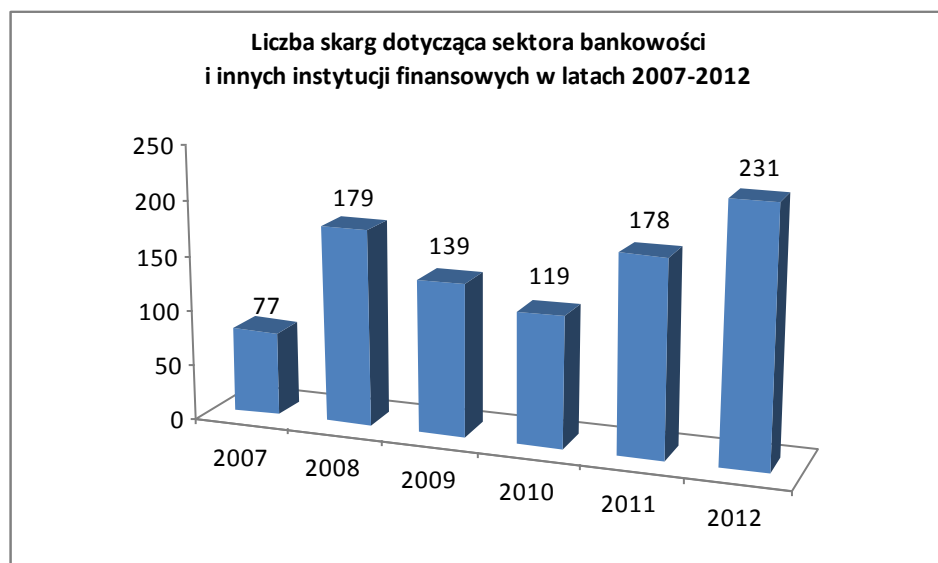
<sup>86</sup> np. DOLiS/DEC-864/12/55792,55796, DOLiS/DEC-488/12/33501,33504.

<sup>87</sup> 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. Rozporządzenie to uchylono z dniem 5 stycznia 2013 r.

<sup>88</sup> np. DOLiS-440-846/12

### 3) Banki i inne instytucje finansowe

W analizowanym 2012 r. do GIODO wpłynęło **231** skarg dotyczących sektora **banków i innych instytucji finansowych**, tj. o 53 więcej niż w roku 2011, w którym skarg tych było 178.



Wykres 17: *Zestawienie porównawcze liczby skarg dotyczących sektora banków i innych instytucji finansowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2012.*

W jednej ze spraw sąd rejonowy wydział cywilny zwrócił się do banku z prośbą o udzielenie informacji na temat tego, czy skarżąca miała lub ma rachunek bieżący, oszczędnościowy bądź lokaty w tym banku, a jeśli tak, to jak wyglądała historia operacji na tym rachunku w okresie ostatnich 3 miesięcy przed rozводом oraz jakie saldo wykazywał ten rachunek na dzień rozvodu. Bank w odpowiedzi na pismo sądu udzielił informacji w szerszym zakresie niż te żądane przez sąd. W związku z powyższym Generalny Inspektor wystąpił do banku z pismem sygnalizującym, że wszelkie działania banku powinny znajdować uzasadnienie w przepisach prawa, w szczególności ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.) oraz ustawy o ochronie danych osobowych<sup>89</sup>. GIODO wskazał, że o ile istniały podstawy do udostępnienia danych w zakresie wskazanym we wniosku sądu, to zdecydowanie nie została spełniona żadna z wymienionych w art. 23 ust. 1 ustawy o ochronie danych osobowych przesłanek legalności udostępnienia pozostałych danych skarżącej. Organ jednocześnie zwrócił uwagę na obowiązek przestrzegania tajemnicy bankowej, ustanowiony w art. 104 ust. 1 Prawa bankowego, zgodnie z którym bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje

<sup>89</sup> Pismo GIODO z dnia 10 stycznia 2012 r. znak: DOLiS-440-566/11/1434/12.

dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.

W omawianym roku sprawozdawczym, do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła duża liczba skarg, w których zakwestionowano legalność działań banków polegającą na przetwarzaniu danych osobowych skarżących w celach archiwalnych, w przypadku odrzucenia przez bank wniosku kredytowego skarżącego. W skutek prowadzonych przez GIODO postępowań ustalono, że zakres tych danych był bardzo szeroki. Wobec tego pojawiły się wątpliwości, czy odpowiada to zakresowi wskazanemu w rozporządzeniu Ministra Finansów z dnia 27 marca 2007 r. w sprawie szczegółowego zakresu przetwarzania informacji dotyczących osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją upoważnioną do udzielania kredytów oraz trybu usuwania tych informacji (Dz. U. z 2007 r. Nr 56, poz. 373). W związku z powyższym Generalny Inspektor zwrócił się do Komisji Nadzoru Finansowego (KNF) z prośbą o wyrażenie opinii w przedmiotowej sprawie i zajęcie stanowiska, czy w jej ocenie przechowywanie informacji zawartych zarówno w dokumentacji papierowej, jak i w systemie informatycznym w szerszym niż ustawowo określonym zakresie, spełnia warunki wskazane w przepisach prawa bankowego lub innych przepisach prawa (np. ustawy o rachunkowości), a jeśli tak, to z jakich konkretnie norm takie uprawnienie należałoby wywodzić<sup>90</sup>. W odpowiedzi Komisja Nadzoru Finansowego wskazała, że podstawę prawną do żądania przez bank dokumentów i informacji pozostających w związku z udzieleniem kredytu stanowi art. 70 ust. 1 Prawa bankowego. W przypadku negatywnego rozpatrzenia wniosku kredytowego, bank nie ma obowiązku, który wynikałby z przepisów prawa, zwrotu przedmiotowych dokumentów. Zdaniem Komisji decyzja o potrzebie i zakresie przechowywania dokumentów po odmowie udzielenia kredytu należy do banku. Wyzbycie się przez bank wszystkich dokumentów (po każdej odmowie udzielenia kredytu) jest ryzykowne i może prowadzić do sytuacji, w której bank nie będzie posiadał dowodów na okoliczność wykazania bezzasadności twierdzeń i roszczeń zgłaszanych przez osoby ubiegające się o kredyt. W ocenie Komisji nie ma przeszkód, by wniosek kredytowy wraz z załącznikami w postaci kopii oryginałów dokumentów, które miały znaczenie dla podjęcia negatywnej decyzji kredytowej, pozostał w banku i podlegał archiwizacji. Komisja wskazała, że niezależnie od celów archiwalnych, dane osobowe osób fizycznych i innych podmiotów, mogą mieć bardzo istotne znaczenie z punktu widzenia oceny ryzyka przez banki i mogą służyć do analizy statystycznej profilu ryzyka. Analizy takie z kolei mogą mieć wpływ na charakter i kierunek prowadzonej przez banki działalności, politykę zarządzania ryzykiem, a w konsekwencji również na zgromadzone w bankach depozyty.

---

<sup>90</sup> Pismo GIODO z dnia 8 czerwca 2012 r. znak: DOLiS-074-9/12/35687.

W analizowanym okresie Generalny Inspektor Ochrony Danych Osobowych zwrócił się o dostosowanie procesu przetwarzania danych osobowych w banku do wymogów ustawy o ochronie danych osobowych poprzez informowanie Biura Informacji Kredytowej S.A. o dokonanych uaktualnieniach lub sprostowaniach przekazanych mu danych osobowych bez zbędnej zwłoki. Generalny Inspektor Ochrony Danych Osobowych wskazywał, że zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Zdaniem organu obowiązek ten oznaczał, że informacje przetwarzane przez administratora danych powinny być zgodnie z prawdą, pełne (kompletne) oraz powinny odpowiadać aktualnemu (najnowszemu) stanowi rzeczy. Zatem obowiązkiem banków było zapewnienie prawdziwości, kompletności i aktualności danych osobowych poprzez poinformowanie Biura Informacji Kredytowej S.A. o zaistniałych zmianach, co powinno nastąpić bez zbędnej zwłoki - jako wyraz szczególnej staranności banku w celu ochrony interesów osób, których dane dotyczą<sup>91</sup>.

Podobnie jak w latach poprzednich, również w 2012 r. do Biura GODO wpływały skargi dotyczące udostępniania danych osobowych podmiotom trzecim, które najczęściej prowadziły działalność windykacyjną<sup>92</sup>. Generalny Inspektor Ochrony Danych Osobowych wydawał wówczas decyzje<sup>93</sup>, w których wskazywał, że administrator danych może przetwarzać dane nie tylko samodzielnie, ale również powierzyć - w drodze pisemnej umowy - ich przetwarzanie innemu podmiotowi, do czego upoważnia go art. 31 ustawy o ochronie danych osobowych. W przypadku gdy administrator skorzysta z upoważnienia wynikającego z brzmienia powołanego przepisu, dochodzi do zlecenia przetwarzania danych „na zewnątrz”. Podmiot, któremu administrator powierzył przetwarzanie danych, może je przetwarzać wyłącznie w przewidzianym umową zakresie i w określonym w umowie celu (art. 31 ust. 2 ustawy). Podmiot ten jest ponadto obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy, oraz spełnić wymagania określone w art. 39a ustawy. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych (art. 31 ust. 3 ustawy). Powierzenie przetwarzania danych dokonane przez administratora na podstawie umowy powierzenia, nie wymaga uzyskania zgody osoby, której dane dotyczą. W niektórych z omawianych spraw dochodziło do sprzedaży wierzytelności<sup>94</sup>. Wówczas GODO w swoich decyzjach wskazywał, że przepisem prawa, z którego wynikał interes prawny w udostępnieniu danych osobowych skarżących

---

<sup>91</sup> por. decyzja GODO z dnia 15 czerwca 2012 r. znak: DOLIS/DEC-536/12/36942,36944.

<sup>92</sup> m.in. DOLIS-440-19/12, DOLIS-440-248/12, DOLIS-440-485/12, DOLIS-440-755/12, DOLIS-440-986/12, DOLIS-440-1117/12.

<sup>93</sup> por. DOLIS/DEC-146/12, DOLIS/DEC-452/12, DOLIS/DEC-446/12.

<sup>94</sup> np. DOLIS-440-986/12

firmom windykacyjnym, był art. 509 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 1964 r. Nr 16, poz. 93 z późn. zm.). W myśl tego przepisu wierzyciel może bez zgody dłużnika przenieść wierzytelność na osobę trzecią (przelew), chyba że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania (§ 1). Wraz z wierzytelnością przechodzą na nabywcę wszelkie związane z nią prawa, w szczególności roszczenie o zaległe odsetki (§ 2). Dla legalności przetwarzania danych osobowych w celu dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej, wystarcza spełnienie przesłanki zawartej w przepisie art. 23 ust. 1 pkt 5 ustawy. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 30 listopada 2004 r. (sygn. akt: II SA/Wa 1057/04) stwierdził bowiem, 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). Zasada ta w pełni odnosi się do podmiotów prawa mających status konsumentów. (...) 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 (będącego konsumentem) 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”*.

W jednej ze spraw dotyczącej wierzytelności ustalono, że skarżący prowadził działalność gospodarczą - wykreśloną obecnie z ewidencji działalności gospodarczej - nie wywiązując się przy tym z zobowiązania wobec spółki zajmującej się usługami telekomunikacyjnymi. Wobec powyższego spółka ta sprzedała wierzytelność podmiotowi zajmującemu się odzyskiwaniem należnych zobowiązań i tym samym doszło do przekazania danych osobowych skarżącego. Spółka zajmująca się windykacją umieściła dane skarżącego na stronie internetowej celem ewentualnej dalszej sprzedaży wierzytelności. Skarżący zażądał od tego podmiotu zaprzestania przetwarzania jego danych osobowych i usunięcia ich ze strony internetowej. W związku z uznaniem przez Generalnego Inspektora Ochrony Danych Osobowych skargi za bezzasadną, skarżący skierował sprawę do Wojewódzkiego Sądu Administracyjnego w Warszawie, który z kolei podzielił stanowisko GODO i oddalił skargę na jego decyzję<sup>95</sup>. WSA w przedmiotowym wyroku wskazał, że cyt.: *„(...) zasadnie w swoich decyzjach zwrócił uwagę organ, że Generalny Inspektor Ochrony Danych Osobowych nie jest władny do dokonywania oceny prawidłowości umów cywilnoprawnych i powstałych na tym gruncie sporów, gdyż właściwość rzeczową w tym zakresie posiadają jedynie sądy powszechne. Organ nie może badać, czy umowa jest ważna i prawnie skuteczna, albowiem w tym przypadku organ administracji publicznej,*

---

<sup>95</sup> Wyrok WSA w Warszawie z dnia 31 maja 2012 r. sygn. akt: II SA/Wa 2367/11.

*jakim niewątpliwie jest GIODO, wykraczałby poza swoje ustawowo określone kompetencje. Dla Generalnego Inspektora Ochrony Danych Osobowych zawarta umowa jest czynnością prawną nie podlegającą jego ocenie, wywołującą skutki prawne do czasu, dopóki nie zostanie zakwestionowana w formie i trybie przewidzianym przez prawo. Powyższy pogląd jest już utrwalony w orzecznictwie sądowoadministracyjnym (por. np. wyrok NSA z 26 maja 2009 r., I OSK 808/08, Lex nr 513109, wyrok WSA w Warszawie z 19 lipca 2007 r., II SA/Wa 678/07, Lex nr 368229). Ustawa o ochronie danych osobowych nie ogranicza swobody prowadzenia działalności gospodarczej przez przedsiębiorców. Zawarcie umowy przelewu wierzytelności wywołuje skutki prawne regulowane zarówno przepisami Kodeksu cywilnego, jak i przepisami ustawy o ochronie danych osobowych. Ocena dopuszczalności, skuteczności, czy też ważności umowy przelewu należy do sądów powszechnych, ewentualnie w niektórych jej aspektach, może być również przedmiotem zainteresowania Prezesa Urzędu Ochrony Konkurencji i Konsumentów. Jest to aspekt cywilnoprawny tej sprawy, który nie może być przedmiotem zainteresowania organu administracji publicznej. Zadanie organu ograniczało się zatem do zbadania w toku postępowania, czy w wyniku zawartej umowy cywilnoprawnej spółka [...] mogła udostępnić dane osobowe skarżącego, zgodnie z przepisami ustawy o ochronie danych osobowych. Generalny Inspektor Ochrony Danych Osobowych wykazał w toku prowadzonego postępowania, iż podjęte przez spółkę [...] działania, w zakresie dokonania cesji wierzytelności, nie pozostawały w sprzeczności z postanowieniami ustawy o ochronie danych osobowych. Organ nie był natomiast uprawniony do badania kwestii istnienia lub nieistnienia wierzytelności, w tym stwierdzenia, czy przedawnienie zobowiązania skutkuje jego wygaśnięciem oraz obowiązku zwrotu długu. (...). Jednocześnie WSA wskazał, że cyt.: „(...) skoro skarżący prowadził działalność gospodarczą jako osoba fizyczna, to po wykreśleniu tej działalności z odpowiedniego rejestru skarżący odpowiada za zobowiązania zaciągnięte w trakcie jej prowadzenia całym majątkiem. W sprawie nie jest sporne, że [...] S.A. miała prawo posiadać i przetwarzać dane osobowe skarżącego w związku z łączącą strony umową o świadczenie usług telekomunikacyjnych (...)”.*

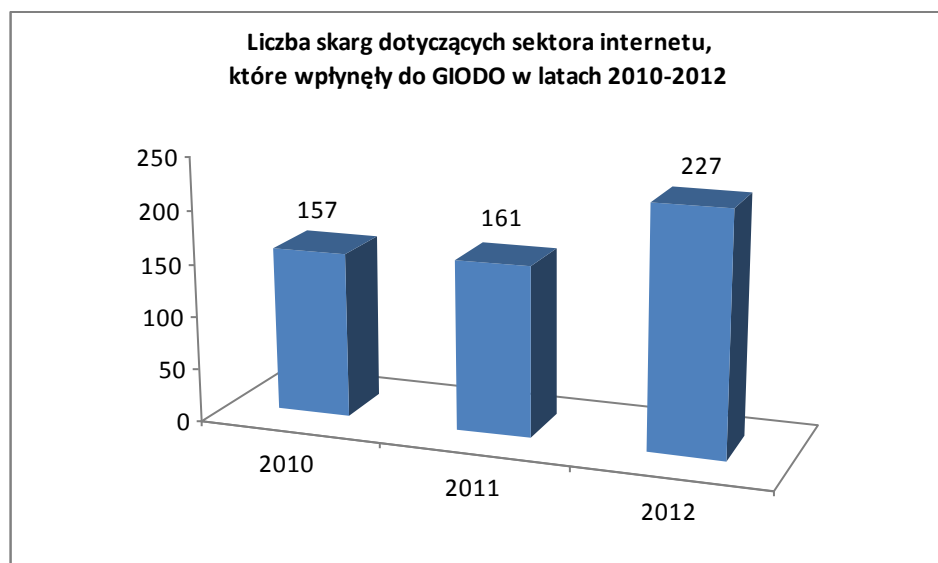
Na zakończenie omawiania przykładów skarg na działalność podmiotów funkcjonujących w obszarze bankowości i różnych innych usług finansowych należy zaznaczyć, że w omawianym roku sprawozdawczym skargi dotyczące przedmiotowego sektora dotyczyły także w znacznej części przetwarzania danych osobowych skarżących w celach marketingowych<sup>96</sup>.

#### **4) Internet**

W 2012 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **227** skarg dotyczących **Internetu**, to jest o 66 więcej w stosunku do roku 2011, w którym skarg tych było 161.

---

<sup>96</sup> DOLiS-440-459/12



**Wykres 18:** *Zestawienie porównawcze liczby skarg dotyczących sektora Internetu, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2012.*

Jedna z takich spraw zawierała wniosek skarżącej<sup>97</sup> - byłej mieszkanki przytuliska dla bezdomnych kobiet – która z okazji jubileuszu istnienia tej placówki opracowała broszury dokumentujące wspomnienia jej mieszkanek. Broszury te skarżąca opatrzyła podpisem „Opracowała Mieszkanka Przytuliska” oraz podpisała swoim imieniem i nazwiskiem. Skarżąca wskazała, że jej praca adresowana była do „rąk prywatnych”, gdy tymczasem bez jej wiedzy trafiła do jednej z bibliotek naukowych. Z uwagi na fakt, że owa biblioteka posiadała internetowy spis dostępnych pozycji, po wpisaniu imienia i nazwiska skarżącej, w wyszukiwarce internetowej wyświetlał się katalog tej biblioteki, zawierający broszurę autorstwa skarżącej. W związku z tym skarżąca wniosła o usunięcie jej danych osobowych z katalogu pozycji znajdujących się na stronie internetowej biblioteki naukowej.

Generalny Inspektor wydał decyzję administracyjną w tej sprawie, nakazując dyrektorowi biblioteki naukowej wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącej, poprzez usunięcie ze strony internetowej danych osobowych w zakresie jej imienia i nazwiska<sup>98</sup>. Organ wskazał, że dyrektor nie mógł przewidzieć, że umieszczenie danych osobowych skarżącej - jako autorki publikacji - w księgozbiorze bibliotecznym, w jakimkolwiek stopniu naruszy jej prawa i wolności. Niewątpliwie dyrektor przetwarzał dane osobowe skarżącej dla wypełnienia prawnie usprawiedliwionego celu, jakim było prowadzenie biblioteki oraz poprawnego tworzenia katalogów księgozbiorów zgodnie z wewnątrznie wprowadzonymi zasadami katalogowania publikacji. Jednocześnie skarżąca osobiście opatrzyła przedmiotową broszurę swoim imieniem i nazwiskiem oraz

<sup>97</sup> DOLiS-440-1197/11

<sup>98</sup> DOLiS/DEC-870/12 dot. DOLiS-440-1197/11.

wykonała jej kopie i musiała się liczyć z możliwością zapoznania się z jej treścią, w tym z jej imieniem i nazwiskiem, przez nieograniczony krąg osób. Jednak Generalny Inspektor wskazał w decyzji, że fakt udostępnienia szerokiemu kręgowi osób - poprzez umieszczenie na przedmiotowej stronie internetowej biblioteki naukowej - informacji dotyczącej przebywania skarżącej w przytulisku dla bezdomnych kobiet, niewątpliwie może mieć realny wpływ na jej sytuację życiową i osobistą. Uznał też, że przetwarzanie danych osobowych autorki publikacji w zaistniałej sytuacji nie było bezwzględnie konieczne. W ocenie Generalnego Inspektora, w pismach kierowanych do dyrektora placówki i do GODO, skarżąca wykazała szczególny charakter swojej sytuacji. Wskazała, że od kilku lat nie mieszka w przytulisku dla bezdomnych kobiet, prowadzi nowe życie i otacza się ludźmi, którzy nie mają świadomości, jak kiedyś wyglądało jej życie. W tej sytuacji, Generalny Inspektor uznał żądanie usunięcia przedmiotowych danych osobowych za uzasadnione w świetle dyspozycji art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych. Zgodnie z treścią tego przepisu, każdej osobie przysługuje prawo do kontroli przetwarzania dotyczących jej danych, zawartych w zbiorach danych, a zwłaszcza prawo do wniesienia - w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 - pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. Jak wskazuje się w doktrynie cyt.: „(...) szczególna sytuacja uzasadniająca zaprzestanie przetwarzania danych osobowych wnioskodawcy wiązać się może z groźbą ujawnienia przez takie przetwarzanie danych związanych ze sferą prywatności lub życia rodzinnego, w przypadku gdy wykorzystywanie tych danych w konkretnej sytuacji nie jest bezwzględnie konieczne. Podjęcie decyzji w sprawie zasadności roszczenia wymaga wyważenia kolidujących ze sobą interesów określonej osoby oraz interesów przemawiających za przetwarzaniem danych. Osoba występująca z roszczeniem powinna wykazać szczególny charakter swojej sytuacji, wyjaśnić, w jakiej mierze jej sytuacja odbiega od sytuacji innych osób, których dane są przetwarzane (...)”<sup>99</sup>.

W 2012 roku Generalny Inspektor Ochrony Danych Osobowych wydał decyzję w sprawie, w której skarżąca wskazała, że pracownik spółki przesłał wiadomość e-mail zawierającą szeroki zakres jej danych osobowych, na nieznany jej adres poczty elektronicznej. Skarżąca wniosła o udostępnienie jej danych osobowych użytkownika przedmiotowego konta e-mail oraz o usunięcie z niego przez portal internetowy korespondencji zawierającej jej dane osobowe. Portal ustalił, iż konto użytkownika nie było używane przez okres ostatnich 24 miesięcy, o czym świadczył brak logowań. Tym samym wszelkie dostarczane na konto wiadomości e-mail nie zostały w tym okresie odczytane. Jednocześnie portal wskazał, że aktualnie zaprzestał dostarczania poczty e-mail na ww. konto, zablokował je administracyjnie i przeznaczył do skasowania. Generalny Inspektor odmówił uwzględniania wniosku skarżącej wskazując, że administrator danych (portal) zasadnie odmówił skarżącej udostępnienia

---

<sup>99</sup> J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz. LEX 2011, Wydanie V.



danych osobowych użytkownika konta e-mail. Skarżąca zwróciła się z wnioskiem o udostępnienie danych kontaktowych, a za takie uznać należy adres e-mail, który przecież był w posiadaniu skarżącej. Mając na względzie, iż wiadomość zawierająca w załączniku dane osobowe skarżącej nie została odczytana przez dysponenta ww. konta, nie było możliwe nieuprawnione wykorzystanie tych danych. Tym samym wniosek skarżącej złożony w tej sprawie nie zasługiwał na uwzględnienie. Ponadto GODO wskazał, że korespondencja znajdująca się w dyspozycji użytkownika będącego właścicielem konta stanowiła jego własność, a administracyjne usunięcie danych z konta mogłoby stanowić czyn zabroniony związany z naruszeniem tajemnicy komunikowania się. Portal nie był zatem uprawniony do ingerowania w zawartość kont użytkowników poczty, w tym do usuwania korespondencji znajdującej się na tych kontach. Usługa poczty elektronicznej należy do kategorii usług świadczonych drogą elektroniczną, do których ma zastosowanie ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204). Podmiotem, do którego należało skierować żądanie w tym zakresie była natomiast spółka, której skarżąca powierzyła swoje dane osobowe i z której konta została wysłana wiadomość do nieuprawnionego odbiorcy.

Przedmiotem kolejnej skargi było udostępnienie przez fundację na stronie internetowej danych osobowych skarżących, w zakresie ich imion, nazwisk oraz miejsc zamieszkania<sup>100</sup>. GODO wydał w przedmiotowej sprawie decyzję administracyjną nakazującą usunięcie danych skarżących, ponieważ dane te zostały zamieszczone na stronie bez ich wiedzy i zgody<sup>101</sup>. Nie wykazano także, aby administrator danych osobowych spełnił inne niż zgoda, przesłanki uzasadniające udostępnienie danych osobowych skarżących na stronie internetowej fundacji. Organ wskazał jednocześnie na art. 26 pkt 1 stanowiący, że administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem. Dodatkowo GODO podkreślił, że za koniecznością usunięcia przez fundację danych osobowych skarżących przemawia regulacja wyrażona w art. 35 ust. 1 ustawy, zgodnie z którą w razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy on danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

---

<sup>100</sup> DOLiS-440-188/12

<sup>101</sup> DOLiS/DEC-869/12 dot. DOLiS-440-188/12.

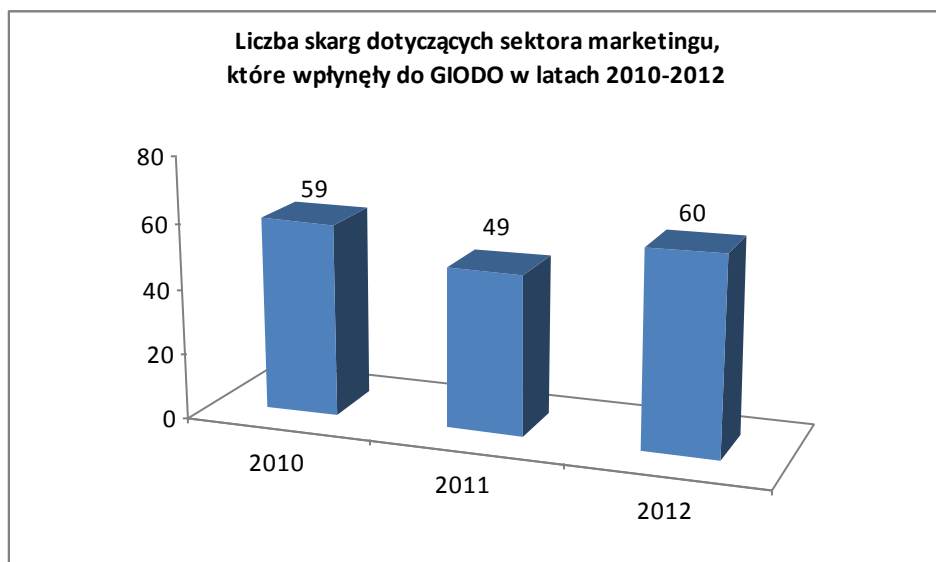
W podsumowaniu stwierdzić należy, że skargi odnoszące się do działalności podmiotów tego sektora dotyczyły w głównej mierze przetwarzania danych osobowych na stronach internetowych bez zgody podmiotu danych oraz zawierały prośby o udostępnienie danych osób, które zamieszczały w Internecie szkalujące treści. W decyzjach wydanych w przedmiotowych sprawach Generalny Inspektor nakazywał udostępnienie danych osobowych w zakresie numerów IP komputera osób, które dokonywały obraźliwych wpisów w Internecie. Wskazywał przy tym, że przyjęcie przeciwnego stanowiska skutkowałoby bezzasadną ochroną przed odpowiedzialnością tego, kto dopuścił się bezprawnej ingerencji w sferę prawnie chronionych interesów drugiej osoby, będąc przekonany o anonimowości, jaką gwarantuje mu sieć. Jak podkreślił Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 3 lutego 2010 r. (sygn. akt II SA/Wa 1598/09) cyt.: „(...) *prawo do swobodnej, anonimowej wypowiedzi, nie może chronić osób, które naruszają prawa innych osób, od odpowiedzialności za wypowiedziane słowa. W sieci nikt nie jest i nie może być anonimowy. Wprawdzie ustalenie tożsamości danej osoby może być utrudnione, jednak z uwagi na to, że każdy komputer zostawia w Internecie ślad – adres IP, za pomocą którego można ustalić komputer, z którego dokonano wpisu, stwarza to możliwość pośredniego ustalenia tożsamości osoby, która dokonała tego wpisu (...)*”<sup>102</sup>.

## 5) Marketing

W analizowanym okresie 2012 roku do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **60** skarg dotyczących sektora **marketingu**. Dla porównania w 2011 r. wpłynęło 49 skarg dotyczących tego obszaru.

---

<sup>102</sup> Przełomowe z punktu widzenia przetwarzania danych osobowych w omawianym sektorze było stwierdzenie Naczelnego Sądu Administracyjnego zawarte w uzasadnieniu do wyroku z dnia 19 maja 2011 r. (sygn. akt: I OSK 1079/10), 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.



Wykres 19: *Zestawienie porównawcze liczby skarg dotyczących sektora marketingu, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2012.*

Najczęściej Generalny Inspektor Ochrony Danych Osobowych wydawał decyzje odmawiające uwzględnienia wniosku<sup>103</sup>. 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. Pomimo tego do skarżących nadal kierowane były drogą telefoniczną oraz poprzez wiadomości tekstowe sms, informacje marketingowe w zakresie możliwości przedłużenia umowy ze spółką, możliwości wymiany telefonu na nowy model, czy skorzystania z nowej oferty spółki. W trakcie postępowań podmioty przyznawały, że wysyłanie treści marketingowych do skarżących następowało w wyniku błędów, które niezwłocznie po interwencji GODO zostały usunięte.

W 2009 r. GODO prowadził sprawę w przedmiocie przetwarzania danych osobowych bez stosownej zgody<sup>104</sup> skarżącej, przez jedną z firm telekomunikacyjnych w celach marketingowych. Spółka wskazała, że wynikało to z błędu w systemie informatycznym i zapewniła, że dane osobowe skarżącej nie były aktualnie przetwarzane w celach marketingowych. W związku z zaistniałą sytuacją, w celu zwiększenia skuteczności ochrony danych osobowych swoich klientów, spółka zastosowała szereg środków technicznych i organizacyjnych, a pracownik odpowiedzialny za błąd przeszedł odpowiednie szkolenie z zakresu ochrony danych osobowych. W 2012 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło kolejne pismo skarżącej z informacją, że spółka w dalszym ciągu przetwarza jej dane osobowe w celach marketingowych, pomimo wcześniejszych

<sup>103</sup> DOLiS/DEC-1007/12 dot. DOLiS-440-223/12, DOLiS/DEC-934/12 dot. DOLiS-440-459/12, DOLiS/DEC-1204/12 dot. DOLiS-440-459/12.

<sup>104</sup> DOLiS-440-341/09

zapewnień. W związku z powyższym GODO wydał decyzję administracją nakazującą przywrócenie stanu zgodnego z prawem, poprzez zaprzestanie przez spółkę przetwarzania danych osobowych skarżącej w celach marketingowych<sup>105</sup>. Pomimo zapewnień spółki, że aktualnie dane osobowe w celach marketingowych nie były przetwarzane, organ ochrony danych osobowych podkreślił, że błąd pracownika (wskazany jako przyczyna niezgodnego z prawem przetwarzania danych skarżącej) zaistniał dwukrotnie – pierwszy raz, kiedy to wskutek nieuwzględnienia w systemie teleinformatycznym braku zgody skarżącej opublikowano w spisie abonentów jej zastrzeżony numer telefonu, natomiast drugi raz - wskutek błędnego włączenia danych skarżącej do akcji marketingowej, mimo złożenia przez nią sprzeciwu wobec przetwarzania danych w tym celu. Przedmiotowych uchybień nie można było uznać za incydentalne. Natomiast działania mające na celu zapobieżenie ich wystąpieniu w przyszłości nie zostały podjęte w adekwatnym zakresie w stosunku do stwierdzonych uchybień w procesie przetwarzania danych osobowych skarżącej. W ocenie GODO należało uznać, że w przedmiotowej sprawie doszło do naruszenia ustawy o ochronie danych osobowych, co skutkowało - stosownie do art. 18 ust. 1 ustawy - wydaniem nakazu przywrócenia stanu zgodnego z prawem. Ponadto Generalny Inspektor Ochrony Danych Osobowych, działając na podstawie art. 17 ust. 2 ustawy, zwrócił się do prezesa spółki o wszczęcie postępowania dyscyplinarnego w stosunku do osoby odpowiedzialnej za przetwarzanie danych osobowych skarżącej pomimo wniesienia przez nią sprzeciwu<sup>106</sup>.

## 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 2011 r. wpłynęło do Biura GODO 81 skarg na podmioty działające w tym obszarze, natomiast w 2012 r. liczba ta była porównywalna – **88 skarg**.

---

<sup>105</sup> DOLiS/DEC-866/12 dot. DOLiS-440-341/09.

<sup>106</sup> DOLiS-440-341/09/55807/12



Wykres 20: *Zestawienie porównawcze liczby skarg dotyczących sektora mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2012.*

Pomimo sygnalizowania tym podmiotom w poprzednich latach konieczności respektowania w ich działalności przepisów ustawy o ochronie danych osobowych, nadal udostępniają one dane osobowe mieszkańców osobom nieupoważnionym, np. poprzez wywieszanie zawiadomienia o porządku obrad walnego zgromadzenia spółdzielni, zawierające dane osobowe ich członków, na tablicach informacyjnych znajdujących się na klatkach schodowych budynków należących do zasobów spółdzielni<sup>107</sup>.

W omawianym roku sprawozdawczym GODO prowadził postępowanie<sup>108</sup>, w wyniku którego ustalił, iż spółdzielnia mieszkaniowa kierowała do mieszkańców korespondencję w niezaklejonych kopertach wielokrotnego użytku, umożliwiając osobom trzecim zapoznanie się z jej treścią. Korespondencja przekazywana była adresatom za pośrednictwem upoważnionego pracownika spółdzielni (sprzątaczkę). Z wyjaśnień spółdzielni wynikało, że takie zachowanie stanowiło praktykę stosowaną przez spółdzielnię. Wobec powyższego GODO zwrócił się do tego podmiotu<sup>109</sup> z pismem sygnalizującym nieprawidłowości, odnosząc się do zasad związanych z bezpieczeństwem danych przetwarzanych w treści korespondencji. Generalny Inspektor wskazał na treść art. 36 ust. 1 ustawy, który stanowi, że administrator danych (w tym przypadku spółdzielnia) obowiązany jest 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

<sup>107</sup> Pismo GODO z dnia 28 listopada 2012 r. znak: DOLiS-440-207/12/72406.

<sup>108</sup> DOLiS-440-452/12

<sup>109</sup> Pismo GODO z dnia 3 października 2012 r., znak: DOLiS-440-452/12/59815.

nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Oznacza to, że spółdzielnia, jako administrator danych członków spółdzielni, obowiązana była podjąć działania mające na celu ochronę ich danych osobowych zawartych w kierowanej do nich korespondencji poprzez doręczanie jej w taki sposób, aby tylko adresat miał do niej dostęp, np. w zaklejonych kopertach. Organ ochrony danych osobowych podkreślił, że korespondencja wraz z danymi podlega ochronie wynikającej nie tylko z ustawy o ochronie danych osobowych, lecz również art. 23 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 1964 r. Nr 16, poz. 93 z późn. zm.), jako dobra osobiste jednostki. GODO wskazał, że dostęp do danych powinny mieć wyłącznie osoby upoważnione i wyłącznie w zakresie niezbędnym do realizacji ich zadań wynikających z umowy zawartej z pracodawcą/administratorem danych osobowych. Jednocześnie każdorazowo korespondencja powinna być dostarczana do adresatów w zamkniętych kopertach, aby uniemożliwić osobie nieuprawnionej dostęp do danych w niej zawartych.

W omawianym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał decyzję<sup>110</sup>, w treści której wskazał, że członek spółdzielni ma prawo do zapoznania się z wszystkimi wymienionymi w art. 30 ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (Dz. U. z 2003 r. Nr 188, poz. 1848 z późn. zm.) kategoriami informacji – zarówno wtedy, gdy zostały one ujęte w rejestrze członków stanowiącym jeden, kompletny, całościowy zestaw danych wymienionych w omawianym przepisie, jak również wówczas, gdy zestaw tych danych został podzielony (jak miało to miejsce w rozpoznawanej sprawie). Zgodnie z art. 30 Prawa spółdzielczego, zarząd spółdzielni prowadzi rejestr członków zawierający ich imiona i nazwiska oraz miejsce zamieszkania (w odniesieniu do członków będących osobami prawnymi - ich nazwę i siedzibę), wysokość zadeklarowanych i wniesionych udziałów, wysokość wniesionych wkładów, ich rodzaj, jeżeli są to wkłady niepieniężne, zmiany tych danych, datę przyjęcia w poczet członków, datę wypowiedzenia członkostwa i jego ustania, a także inne dane przewidziane w statucie. Członek spółdzielni, jego małżonek i wierzyciel członka lub spółdzielni ma prawo przeglądać rejestr. W wydanej w tej sprawie decyzji Generalny Inspektor Ochrony Danych Osobowych podkreślił także, że art. 30 Prawa spółdzielczego wskazuje na zakres obowiązkowo przetwarzanych przez każdą spółdzielnię i dostępnych dla każdego członka spółdzielni danych osobowych jej członków. Z punktu widzenia przepisów ustawy o ochronie danych osobowych wszystkie wskazane informacje (o ile stanowią dane osobowe) – bez względu na to czy zostały ujęte w jeden kompleksowy zestaw, czy w szereg zestawów – stanowią jeden zbiór danych osobowych (art. 7 pkt 1 ustawy o ochronie danych osobowych). Art. 30 Prawa spółdzielczego kształtuje po stronie każdego członka spółdzielni prawo do zapoznania się z wymienionymi w nim kategoriami danych osobowych (któremu to uprawnieniu odpowiada

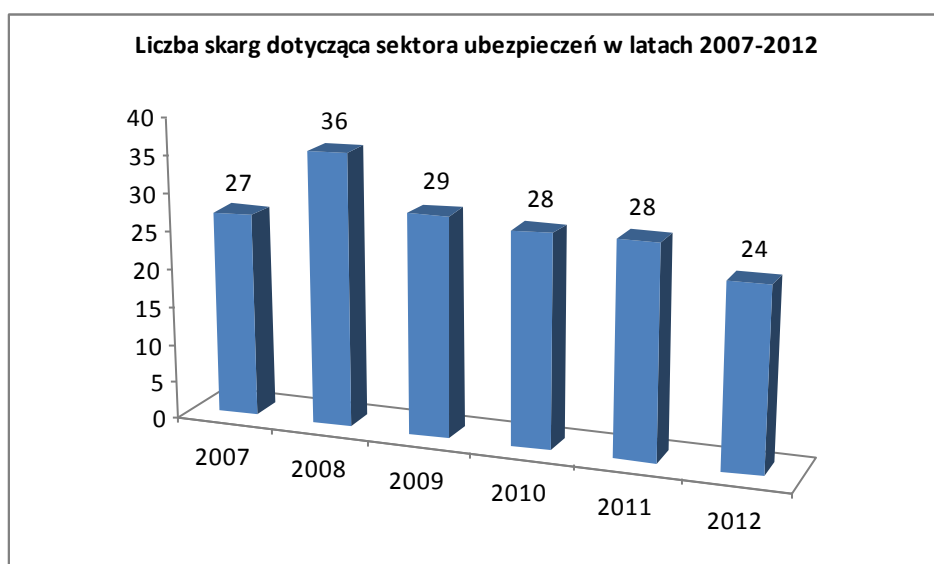
---

<sup>110</sup> DOLiS/DEC-389/12 dot. DOLiS-440-722/11.

spoczywający na spółdzielni obowiązek ich udostępnienia na rzecz uprawnionych) – stanowiąc przepis prawa, o którym mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Wbrew stanowisku spółdzielni, realizacja powyższego uprawnienia nie jest uwarunkowana wskazaniem przez skarżących dodatkowego celu pozyskania wnioskowanych danych, czy interesu prawnego uzasadniającego ich żądanie. Do zdania organu ochrony danych osobowych przychylił się także Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 29 listopada 2012 r.<sup>111</sup> oddalając skargę spółdzielni na decyzję Generalnego Inspektora Ochrony Danych Osobowych.

#### 7) Ubezpieczenia społeczne, majątkowe i osobowe

W 2012 r. do GIODO wpłynęły **24 skargi dotyczące sektora ubezpieczeń społecznych, majątkowych i osobowych**. Liczba ta jest porównywalna z poprzednim rokiem sprawozdawczym, w którym skarg tych było 28.



Wykres 21: *Zestawienie porównawcze liczby skarg na podmioty działające w sektorze ubezpieczeń społecznych, majątkowych i osobowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2012.*

W omawianym roku sprawozdawczym GIODO prowadził postępowanie administracyjne, w którym skarżący zawarł umowę ubezpieczenia w zakresie obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych. Z uwagi na to, iż do ostatniego dnia trwania umowy ubezpieczyciela nie wpłynęło pisemne wypowiedzenie ww. umowy, na zasadzie „automatyzmu”, wyrażonej w art. 28 ust. 1 ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli

<sup>111</sup> Wyrok WSA w Warszawie z dnia 29 listopada 2012 r. sygn. akt II SA/Wa 1343/12.

Komunikacyjnych (Dz. U. Nr 124, poz. 1152 z późn. zm.), pomiędzy ubezpieczycielem a skarżącym została zawarta kolejna umowa ww. rodzaju. Skarżący wskazał, że wysłał pismo do ubezpieczyciela, zawierające – w jego ocenie - odstąpienie od przedmiotowej umowy. Z uwagi na fakt, że skarżący wysłał owe pismo listem zwykłym, natomiast ubezpieczyciel zaprzeczył jakoby otrzymał przedmiotowe wypowiedzenie, w aktach sprawy nie znajdował się żaden dowód potwierdzający słuszność twierdzeń skarżącego. Jednocześnie skarżący zażądał, aby ubezpieczyciel zaprzestał przetwarzania jego danych osobowych w celu dochodzenia zapłaconia zaległej składki z tytułu umowy ubezpieczenia. Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną<sup>112</sup> odmawiającą uwzględnienia wniosku skarżącego. Zgodnie z art. 28 ust. 1 o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, jeżeli posiadacz pojazdu mechanicznego nie później niż na jeden dzień przed upływem okresu 12 miesięcy, na który umowa ubezpieczenia OC posiadaczy pojazdów mechanicznych została zawarta, nie powiadomi na piśmie zakładu ubezpieczeń o jej wypowiedzeniu, uważa się, że została zawarta następna umowa na kolejne 12 miesięcy. Wobec powyższego, organ w swojej decyzji wskazał, że przetwarzanie danych osobowych skarżącego przez ubezpieczyciela - zarówno dla celów związanych z możliwością zgłoszenia pod adresem wskazanego ubezpieczyciela roszczeń wynikających z zawartej w przeszłości ze skarżącym umowy ubezpieczenia, jak i w celu dochodzenia w stosunku do skarżącego roszczeń ubezpieczyciela o zapłatę składki należnej z tytułu ww. umowy - należy uznać za uprawnione (realizowane na zasadach określonych w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych). Podkreślić należy, że kwestie istnienia bądź nieistnienia pomiędzy skarżącym a ubezpieczycielem określonego stosunku prawnego (wynikającego z umowy ubezpieczenia), i w konsekwencji wynikających stąd praw, wzajemnych obowiązków i roszczeń ww. podmiotów, nie podlega weryfikacji Generalnego Inspektora Ochrony Danych Osobowych.

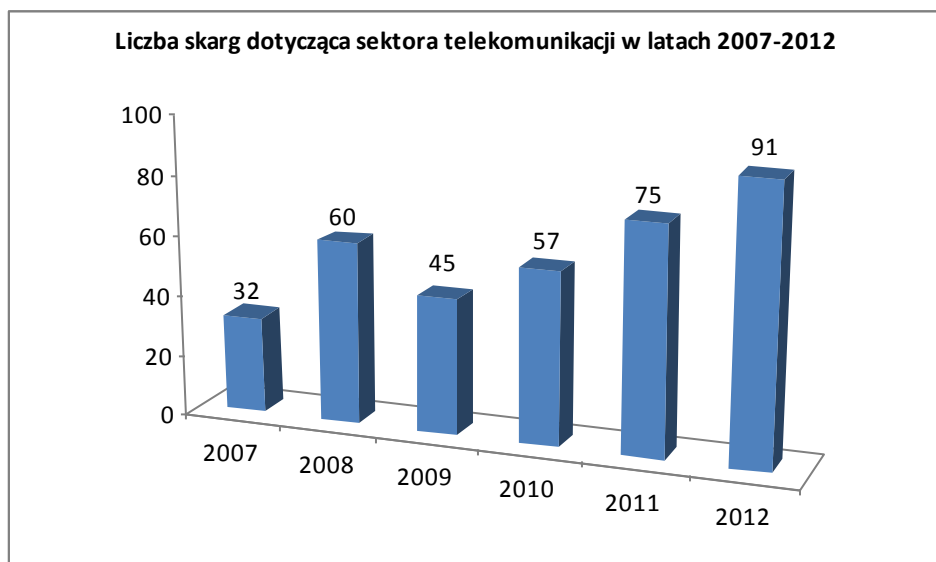
## **8) Telekomunikacja**

W 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **91 skarg dotyczących działalności telekomunikacyjnej**. W porównaniu z rokiem 2011 r., w którym wpłynęło 75 skarg z tego zakresu, stanowi to wzrost o ponad 21 %.

---

<sup>112</sup> DOLiS/DEC-87/12 dot. DOLiS-440-112/11.





**Wykres 22:** *Zestawienie porównawcze liczby skarg na podmioty działające w sektorze telekomunikacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2012.*

Nadawcą jednej z nich<sup>113</sup> był komendant straży miejskiej, który poinformował o prowadzonym postępowaniu wyjaśniającym w sprawie o wykroczenie przeciwko domniemanemu sprawcy, który umieścił ogłoszenie w miejscu publicznym do tego nieprzeznaczonym. Zwrócił się więc do operatora telekomunikacyjnego o udostępnienie danych osobowych nadawcy ogłoszenia. Operator odmówił powołując się na obowiązek zachowania tajemnicy telekomunikacyjnej wynikającej z art. 159 Prawa telekomunikacyjnego<sup>114</sup>. Generalny Inspektor Ochrony Danych Osobowych w swojej decyzji<sup>115</sup> nakazał operatorowi telekomunikacyjnemu udostępnienie komendantowi straży miejskiej danych osobowych abonenta telefonu, w zakresie jego imienia, nazwiska oraz adresu zamieszkania, wskazując, że realizacja przez straż miejską jej ustawowych zadań<sup>116</sup> wymaga wykorzystywania informacji o osobach, których działania te dotyczą. W przedmiotowej sprawie straż miejska wykonuje zadania w zakresie ochrony porządku publicznego. Do wypełnienia zadania realizowanego dla dobra publicznego niezbędne jest ustalenie sprawcy wykroczenia, a następnie skierowania do sądu wniosku o ukaranie. Dobra publiczne jest wartością, którą spółka winna wziąć pod uwagę w kontekście realizacji obowiązku ochrony danych abonenta na gruncie przepisów ustawy Prawo telekomunikacyjne i wyważyć wyższość dobra publicznego nad prawem jednostki do decydowania o sposobie przetwarzania dotyczących jej danych osobowych. Oznacza to, iż straż miejska, na mocy stosownych przepisów rangi ustawowej, ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie

<sup>113</sup> DOLiS-440-802/12

<sup>114</sup> Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, (Dz. U. 2004 r. Nr 171, poz. 1800 z późn. zm.).

<sup>115</sup> DOLiS/DEC-1051/12 dot. DOLiS-440-802/12.

<sup>116</sup> Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 1997 r. Nr 123, poz. 779 z późn. zm.) oraz ustawa z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. 2008 r. Nr 133, poz. 848 z późn. zm.).

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 ten podmiot<sup>117</sup>.

W omawianym roku sprawozdawczym do Biura Generalnego Inspektora Ochrony Danych Osobowych wpływały także skargi dotyczące odmowy udostępnienia przez przedsiębiorcę telekomunikacyjnego, danych osobowych w zakresie numeru IP komputera, z którego dokonano wpisów naruszających prawa wnioskujących. W tych konkretnych przypadkach skarg GODO wydawał decyzje odmawiające uwzględnienia wniosku skarżących<sup>118</sup>. W przedmiotowych decyzjach wskazywał, że choć ustawa o ochronie danych osobowych stanowi podstawowy akt prawny regulujący kwestię ochrony danych osobowych, jednakże jest ona uzupełniana licznymi przepisami szczególnymi. Ustawodawca chcąc rozwiązać kwestię zbiegu przepisów uznał, że 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 (art. 5 ustawy o ochronie danych osobowych).

W opinii Generalnego Inspektora taka sytuacja miała miejsce w przedmiotowych sprawach. Generalny Inspektor wskazał, że w art. 159 ust. 1 Prawa telekomunikacyjnego statuowana jest tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana „*tajemnicą telekomunikacyjną*”, obejmująca swoim zakresem m.in. dane dotyczące użytkownika (pkt 1). Stosownie do brzmienia art. 159 ust. 2 Prawa telekomunikacyjnego, zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że: będzie to przedmiotem usługi lub będzie to niezbędne do jej wykonania (pkt 1), nastąpi za zgodą nadawcy lub odbiorcy, których dane te dotyczą (pkt 2), dokonanie tych czynności jest niezbędne w celu rejestrowania komunikatów i związanych z nimi danych transmisyjnych, stosowanego w zgodnej z prawem praktyce handlowej dla celów zapewnienia dowodów transakcji handlowej lub celów łączności w działalności handlowej (pkt 3), będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi (pkt 4). W myśl art. 159 ust. 3 Prawa telekomunikacyjnego, z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej. Zgodnie z art. 161 ust. 1 ww. ustawy, z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „*przetwarzaniem*”, dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach

---

<sup>117</sup> 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.

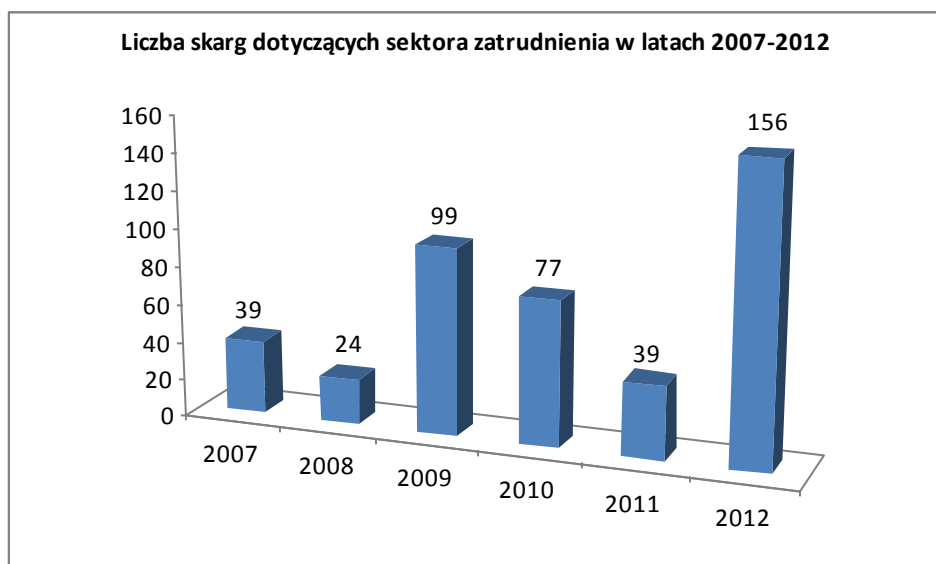
<sup>118</sup> por. DOLiS/DEC-154/12 dot. DOLiS-440-874/11, DOLiS/DEC-686/12 dot. DOLiS-440-653/11.

jest dopuszczalne jedynie na podstawie przepisów ustawowych. W przedmiotowych decyzjach Generalny Inspektor wskazywał, że powołane przepisy art. 159 oraz art. 161 ust. 1 Prawa telekomunikacyjnego przewidują dalej idącą ochronę danych osobowych, o których mowa w art. 159 ust. 1 wspomnianego aktu prawa. W takiej sytuacji, zgodnie z regułą wyrażoną w art. 5 ustawy o ochronie danych osobowych, zastosowanie znajdują przepisy przewidujące dalej idącą ochronę danych osobowych.

Z przedstawionych powyżej względów kierowane pod adresem Generalnego Inspektora Ochrony Danych Osobowych wnioski o nakazanie przedsiębiorcy telekomunikacyjnemu udostępnienia określonych danych osobowych abonenta, nie mogły zostać uwzględnione. Udostępnieniu przedmiotowych danych sprzeciwiały się zarówno powołane przepisy dotyczące tajemnicy telekomunikacyjnej, jak również art. 5 ustawy o ochronie danych osobowych.

## 9) Zatrudnienie

W 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **156 skarg dotyczących podmiotów sektora zatrudnienia**. W porównaniu z poprzednim rokiem sprawozdawczym, w którym wpłynęło ich jedynie 38, stanowi to znaczny, bo ponad czterokrotny wzrost liczby skarg na podmioty działające w tym obszarze.



Wykres 23: *Zestawienie porównawcze liczby skarg dotyczących sektora zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2012.*

Przyczyną tak znacznego wzrostu liczby skarg dotyczących tego sektora było to, że większość z nich dotyczyła analogicznego stanu faktycznego. Pracownicy jednego z przedsiębiorstw złożyli do GIODO skargi, że z siedziby ich pracodawcy, osoby reprezentujące spółkę (z którą – ich zdaniem -

pracodawca ten jest w konflikcie), zabrały „akta osobowe i rzeczy osobiste” i przetrzymują je w miejscu im nieznanym. W przedmiotowych sprawach Generalny Inspektor Ochrony Danych Osobowych w dalszym ciągu prowadzi postępowanie wyjaśniające.

W omawianym 2012 roku Generalny Inspektor wydał decyzję administracyjną<sup>119</sup> nakazującą pracodawcy usunięcie uchybień przy przetwarzaniu danych osobowych pracowników. Uchybienia te polegały na pozyskiwaniu informacji o osobach korzystających z ochrony związku zawodowego. W przedmiotowej decyzji GODO wskazał, że stosownie do art. 30 ust. 2<sup>1</sup> ustawy o związkach zawodowych, w indywidualnych sprawach ze stosunku pracy, w których przepisy prawa pracy zobowiązują pracodawcę do współdziałania z zakładową organizacją związkową, pracodawca jest obowiązany zwrócić się do tej organizacji o informację o pracownikach korzystających z jej ochrony, zgodnie z przepisami ust. 1 i 2. Nieudzielenie tej informacji w ciągu 5 dni zwalnia pracodawcę od obowiązku współdziałania z zakładową organizacją związkową w sprawach dotyczących tych pracowników. GODO zwrócił uwagę, że ww. przepis stanowi rozwinięcie zasady wyrażonej w art. 23<sup>2</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.). W świetle tej zasady, jeżeli przepisy prawa pracy przewidują współdziałanie pracodawcy z zakładową organizacją związkową w indywidualnych sprawach wynikających ze stosunku pracy, wówczas pracodawca ma obowiązek współdziałania z tym podmiotem (jako że reprezentuje pracownika z tytułu jego członkostwa w tym związku), albo wyrażenia zgody na obronę praw pracownika niezrzeszonego - zgodnie z ustawą o związkach zawodowych. W przedmiotowej decyzji GODO wskazał, że przepisy art. 30 ust. 2<sup>1</sup> ustawy o związkach zawodowych oraz art. 23<sup>2</sup> Kodeksu pracy (K.p.), nie mogą stanowić podstawy do pozyskiwania przez pracodawcę od związku danych osobowych wszystkich pracowników korzystających z jego ochrony. Przepisy te bowiem odnoszą się do ochrony stosunku pracy indywidualnego pracownika. W przypadku wypowiedzenia wynikających z umowy warunków pracy i płacy, ochronę taką zapewnia art. 42 § 1 K.p. GODO podkreślił, że pozyskiwanie informacji o korzystaniu przez pracownika z ochrony związkowej było uzasadnione w razie zamiaru wypowiedzenia warunków pracy i płacy konkretnemu pracownikowi lub rozwiązania umowy o pracę z konkretnym pracownikiem. Dlatego brak było podstaw do pozyskiwania przez pracodawcę od związku danych osobowych we wskazanym zakresie, w odniesieniu do wszystkich pracowników korzystających z ochrony związku. Zwłaszcza w sytuacji, gdy nie byli oni objęci zamiarem pracodawcy wypowiedzenia im warunków zatrudnienia lub rozwiązania z nimi umów o pracę.

W ocenie Generalnego Inspektora pozyskiwanie w ten sposób przedmiotowych danych naruszało określoną w art. 26 ust. 1 pkt 3 ustawy zasadę adekwatności. Powołany przepis stanowi, iż administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony

---

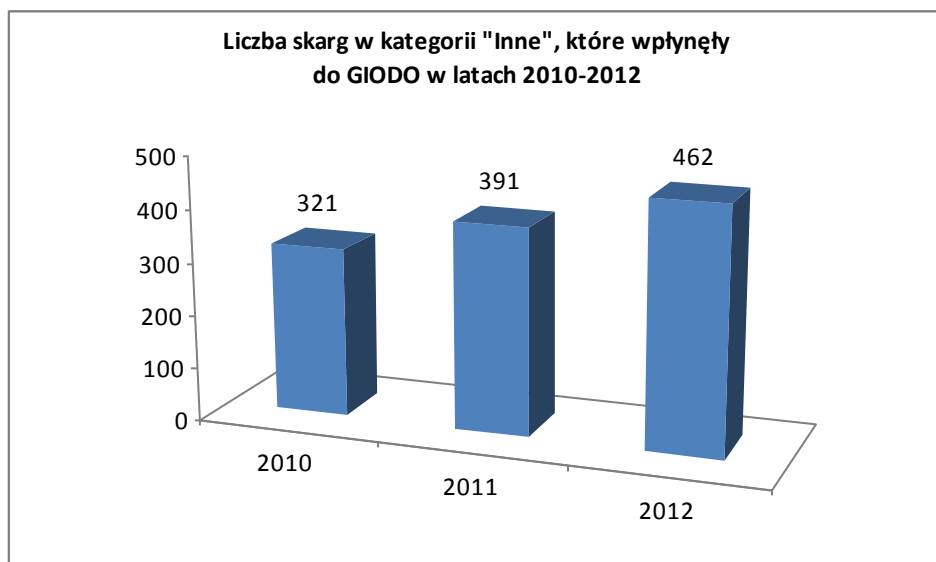
<sup>119</sup> DOLiS/DEC-899/12 dot. DOLiS-440-1059/11.

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 realizacja przez związki zawodowe tego typu wniosków pracodawców skutkowałaby pozyskaniem danych osobowych objętych ochroną związkową również na zapas, co w świetle przepisów ustawy jest niedopuszczalne.

Podkreślić należy, że Generalny Inspektor nie kwestionuje prawa pracodawców do pozyskiwania informacji o pracownikach korzystających z ochrony związkowej, lecz jedynie sposób realizacji tego prawa. Zdaniem Generalnego Inspektora pracodawcy powinni mieć na uwadze wymagania określone przepisami ustawy o ochronie danych osobowych, w tym określoną w art. 26 ust. 1 pkt 2 ustawy zasadę celowości. Stwierdzić należy, że poza cel gromadzenia danych, jakim jest korzystanie z ochrony związku zawodowego - wskazany w przypadkach określonych w przepisach K.p. - wykracza pozyskiwanie danych osobowych wszystkich pracowników korzystających z ochrony związkowej za pomocą ich imiennego wykazu. Wskazuje na to również uchwała Sądu Najwyższego z dnia 24 stycznia 2012 r. w sprawie o sygn. akt III PZP 7/11, w której Sąd Najwyższy, przyjmując pogląd wyrażony przez sądy administracyjne, stwierdził, iż *„Nieudzielenie przez zakładową organizację związkową żądanej przez pracodawcę informacji o pracownikach korzystających z jej obrony, nie zwalnia pracodawcy z obowiązku zawiadomienia organizacji związkowej o zamiarze wypowiedzenia pracownikowi umowy o pracę, jeżeli nieudzielenie tej informacji było uzasadnione ochroną danych osobowych (art. 38 § 1 K.p., art. 30 ust. 2<sup>1</sup> ustawy z dnia 23 maja 1991 r. o związkach zawodowych, jednolity tekst: Dz. U. z 2001 r. Nr 79, poz. 854 z późn. zm. oraz art. 23 ust. 1 pkt 2 i art. 26 ust. 1 pkt 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jednolity tekst: Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)”*.

## 10) Inne

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2012 r. wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej przedstawionych kategorii spraw. W roku 2012 ich liczba wyniosła **462**. Analizując przedstawione poniżej zestawienie porównawcze liczby skarg w kategorii „Inne”, które wpłynęły do GIODO w latach 2010-2012 zauważyć należy, że co roku liczba tych skarg zwiększa się o około 70 w stosunku do roku poprzedniego.



Wykres 24: *Zestawienie porównawcze liczby skarg z sektora „Inne”, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010–2012.*

W tym miejscu warto wskazać, że w omawianym sektorze występowały – podobnie jak w latach poprzednich - skargi zawierających zarzut przetwarzania danych osobowych przez proboszczów **parafii Kościoła Katolickiego**<sup>120</sup>. Skarżący wskazywali w nich, iż pomimo złożenia oświadczenia o wystąpieniu z Kościoła Katolickiego, nie została o tym fakcie zamieszczona stosowna adnotacja w księdze chrztów. Generalny Inspektor Ochrony Danych Osobowych zwracał się w poszczególnych sprawach o wyjaśnienia do odpowiednich podmiotów przetwarzających dane członków lub byłych członków Kościoła Katolickiego. Z uzyskanych wyjaśnień wynikało, że osoby skarżące były wciąż członkami Kościoła Katolickiego, ponieważ nie przeszły procedury apostazji. W związku z powyższym 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<sup>121</sup>. Wiele z tych rozstrzygnięć zostało poddanych kontroli sądowej wskutek ich zaskarżenia do WSA w Warszawie. W wydanych w tych sprawach wyrokach<sup>122</sup> sądy podzieliły zdanie organu ochrony danych osobowych.

W innej sprawie Generalny Inspektor prowadził postępowanie administracyjne, w toku którego ustalono, że dokonano wszelkich procedur przewidzianych prawem kościelnym i odnotowano fakt

<sup>120</sup> m. in.: DOLiS-440-21/12, DOLiS-440-81/12, DOLiS-440-84/12, DOLiS-440-409/12, DOLiS-440-741/12, DOLiS-440-864/11.

<sup>121</sup> m. in. DOLiS/DEC-1086/12, DOLiS/DEC- 1087/12, DOLiS/DEC- 170/12, DOLiS/DEC- 229/12, DOLiS/DEC- 238/12, DOLiS/DEC- 253/12.

<sup>122</sup> wyrok WSA w Warszawie z dnia 15 lutego 2012 r. sygn. akt II SA/Wa 2244/11, wyrok WSA w Warszawie z dnia 28 maja 2012 r. sygn. akt II SA/Wa 340/12, wyrok WSA w Warszawie z dnia 18 października 2012 r. sygn. akt II SA/Wa 442/12, wyrok WSA w Warszawie z dnia 22 października 2012 r. sygn. akt II SA/Wa 1295/12, wyrok WSA w Warszawie z dnia 26 października 2012 r. sygn. akt II SA/Wa 900/12.

apostazji skarżącego w metryce jego chrztu i księdze ślubu. Natomiast nie zamieszczono tej informacji w metrykach chrztu dzieci skarżącego. Parafia wskazała, że dzieci skarżącego były już dorosłe i tylko one miały prawo dostępu do swoich aktów chrztu i dokonywania w nich zmian. Organ ochrony danych osobowych wskazał w decyzji, że z uwagi na treść art. 43 ust. 2 ustawy o ochronie danych osobowych, nie był uprawniony do wydania w przedmiotowej sprawie decyzji administracyjnej rozstrzygającej, co do istoty sprawy, czy też przeprowadzenia czynności kontrolnych. Wobec powyższego organ umorzył postępowanie. Skarżący złożył na tę decyzję skargę do Wojewódzkiego Sądu Administracyjnego w Warszawie, który w wyroku z dnia 26 października 2012 r.<sup>123</sup> wskazał, że cyt.: „(...) Kościół Katolicki posiada autonomię w zakresie wykonywania władzy duchownej i jurysdykcyjnej oraz zarządza swoimi sprawami. Zasadnie zatem Generalny Inspektor Ochrony Danych Osobowych uznał, iż z uwagi na treść art. 43 ust. 2 ustawy o ochronie danych osobowych, nie był uprawniony do wydania w przedmiotowej sprawie decyzji administracyjnej rozstrzygającej co do istoty, czy też przeprowadzenia czynności kontrolnych. Mógł jedynie żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przeszukiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego i takie działanie w niniejszej sprawie niewątpliwie podjął. (...)”. „(...) przetwarzanie przez Kościół Katolicki danych osobowych jego wiernych nie korzysta z ochrony państwowej, a przez to także i wspólnotowej (...)”.

#### **4. Egzekwowanie obowiązków o charakterze niepieniężnym określonych w decyzjach administracyjnych GODO**

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, w art. 12 pkt 3 zostało nałożone na Generalnego Inspektora Ochrony Danych Osobowych nowe zadanie - zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych, 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.). Zgodnie z art. 2 § 1 tej ustawy, egzekucji administracyjnej podlegają obowiązki z zakresu ochrony danych osobowych nakładane w drodze decyzji Generalnego Inspektora Ochrony Danych Osobowych. Generalny Inspektor uznany został za organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym<sup>124</sup>, a obowiązki z zakresu

---

<sup>123</sup> wyrok WSA w Warszawie z dnia 26 października 2012 r. sygn. akt II SA/Wa 900/12.

<sup>124</sup> art. 20 § 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji.

ochrony danych osobowych nakładane w drodze wydawanych przez niego decyzji, zostały dodane do katalogu obowiązków podlegających egzekucji administracyjnej<sup>125</sup>.

W celu realizacji tego zadania Generalny Inspektor podjął stosowne działania organizacyjne<sup>126</sup> oraz wprowadził wewnętrzne procedury<sup>127</sup> dla zapewnienia realizacji wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych.

Zarządzeniem Nr 1/2012 z dnia 4 stycznia 2012 r. w sprawie wprowadzenia Regulaminu Organizacyjnego Biura GIODO, w Załączniku Nr 1, powołał nową komórkę organizacyjną – Zespół do Spraw Egzekucji Administracyjnej (ZEA) - i określił jej zakres działania. W § 24 wspomnianego dokumentu stwierdza się, że do podstawowych zadań Zespołu należy między innymi wykonywanie zadań związanych z wszczynaniem i prowadzeniem z upoważnienia Generalnego Inspektora, postępowań egzekucyjnych obowiązków o charakterze niepieniężnym, a w szczególności wystawianie tytułów wykonawczych i wszczynanie postępowań egzekucyjnych, wydawanie postanowień o nałożeniu/umorzeniu grzywny w celu przymuszenia, wydawanie postanowień w sprawie zgłaszanych zarzutów, a także opracowywanie projektów rozstrzygnięć wskutek wniesionych przez zobowiązanych skarg, zażaleń i wniosków na czynności egzekucyjne. W zakresie wykonywania ww. zadań i monitorowania postępowań egzekucyjnych, Generalny Inspektor Ochrony Danych Osobowych współpracuje z naczelnikami urzędów skarbowych.

Procedurę działania Biura GIODO w zakresie wymienionych wyżej zadań komórki egzekucyjnej GIODO, określają „Zasady prowadzenia egzekucji administracyjnej obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych GIODO”, wprowadzone w życie Zarządzeniem Nr 16/2012 z dnia 16 lipca 2012 r.<sup>128</sup>

W postępowaniu egzekucyjnym obowiązków o charakterze niepieniężnym z zakresu wykonania przepisów o ochronie danych osobowych nakładanych w drodze decyzji, Generalny Inspektor Ochrony Danych Osobowych jest wierzycielem i organem egzekucyjnym. Natomiast w zakresie należności

---

<sup>125</sup> art. 2 § 1 pkt 12 cyt. w. ustawy o postępowaniu egzekucyjnym w administracji.

<sup>126</sup> Zarządzenie Nr 1/2012 z dnia 04 stycznia 2012 r. w sprawie wprowadzenia Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych wraz z Załącznikiem Nr 1.

<sup>127</sup> Zarządzenie nr 16/2011 z dnia 15 lipca 2011 r. Generalnego Inspektora Ochrony Danych Osobowych w sprawie wprowadzenia zasad prowadzenia egzekucji administracyjnej obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych Generalnego Inspektora Ochrony Danych Osobowych; Zarządzenie nr 17/2011 z dnia 15 lipca 2011 r. Generalnego Inspektora Ochrony Danych Osobowych w sprawie określenia wzorów druków stosowanych w związku z prowadzeniem przez Generalnego Inspektora Ochrony Danych Osobowych egzekucji administracyjnej obowiązków z zakresu ochrony danych osobowych; Zarządzenie nr 15/2012 z dnia 16 lipca 2012 r. Generalnego Inspektora Ochrony Danych Osobowych w sprawie zmiany Zarządzenia nr 17/2011 z dnia 15 lipca 2011 r. Generalnego Inspektora Ochrony Danych Osobowych w sprawie określenia wzorów druków stosowanych w związku z prowadzeniem przez Generalnego Inspektora Ochrony Danych Osobowych egzekucji administracyjnej obowiązków z zakresu ochrony danych osobowych; Zarządzenie nr 16/2012 z dnia 16 lipca 2012 r. Generalnego Inspektora Ochrony Danych Osobowych w sprawie zmiany Zarządzenia nr 16/2011 z dnia 15 lipca 2011 r. Generalnego Inspektora Ochrony Danych Osobowych w sprawie wprowadzenia zasad prowadzenia egzekucji administracyjnej obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych Generalnego Inspektora Ochrony Danych Osobowych.

<sup>128</sup> Zarządzenie Nr 16/2012 Generalnego Inspektora Ochrony Danych Osobowych z dnia 16 lipca 2012 r. w sprawie zmiany Zarządzenia Nr 16/2011 Generalnego Inspektora Ochrony Danych Osobowych z dnia 15 lipca 2011 r. w sprawie wprowadzenia zasad prowadzenia egzekucji administracyjnej obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych Generalnego Inspektora Ochrony Danych Osobowych.



pieniężnych (koszty upomnienia, koszty egzekucyjne, grzywna w celu przymuszenia) organem egzekucyjnym jest naczelnik urzędu skarbowego, zaś GIODO - wierzycielem.

Prowadząc postępowania egzekucyjne Generalny Inspektor przyjął założenie, że będzie podejmował czynności zmierzające do zastosowania środków egzekucyjnych wobec każdego zobowiązanego, na którego taki obowiązek został nałożony w drodze decyzji administracyjnej, a który od wykonania takiego obowiązku się uchyla.

Należy w tym miejscu nadmienić, że od dnia wejścia w życie znowelizowanej ustawy o ochronie danych osobowych, decyzje GIODO zostały opatrzone w dodatkowe pouczenie, którego celem było uświadomienie stronom decyzji, że niewykonanie w terminie nakazów w niej określonych będzie skutkowało podjęciem przez organ ds. ochrony danych osobowych działań, mających na celu zapewnienie ich wykonania przez zastosowanie środków egzekucyjnych przewidzianych we wspomnianej ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji. Ponadto przed skierowaniem sprawy na drogę postępowania egzekucyjnego, każdy zobowiązany wzywany jest do dobrowolnego wykonania nałożonego na niego obowiązku. Dopiero po bezskutecznym wezwaniu wszczynane było postępowanie egzekucyjne. W trakcie postępowania egzekucyjnego stosowane są tylko środki egzekucyjne, przewidziane w ustawie o postępowaniu egzekucyjnym w administracji. Co więcej, przy wyborze tych środków kierowano się zasadą najmniejszej uciążliwości dla zobowiązanych.

Egzekucji administracyjnej podlegają wszystkie decyzje administracyjne Generalnego Inspektora nakładające na strony obowiązek (nakaz) do wykonania, które są ostateczne oraz te, którym nadano rygor natychmiastowej wykonalności. Jeżeli decyzja administracyjna zawierała postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlegał egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek do wykonania nakładany na stronę (zobowiązanego) może polegać na usunięciu uchybień, uzupełnieniu, uaktualnieniu, sprostowaniu, udostępnieniu lub nieudostępnieniu danych osobowych, zastosowaniu dodatkowych środków zabezpieczających zgromadzone dane osobowe, wstrzymaniu przekazywania danych osobowych do państwa trzeciego, zabezpieczeniu danych lub przekazaniu ich innym podmiotom, na usunięciu danych osobowych, czy wreszcie na ponownym zgłoszeniu zbioru danych osobowych do rejestracji Generalnemu Inspektorowi wolnego od wad, które były powodem odmowy jego rejestracji.

Dla przykładu, po przeprowadzeniu postępowania rejestrowych wszczętych nie wcześniej niż dnia 7 marca 2011 r. w 2012 r., Generalny Inspektor Ochrony Danych Osobowych wydał 57 decyzji zawierających nakazy wynikające z art. 44 ust. 2 ustawy o ochronie danych osobowych, których projekty zostały opracowane w Departamencie Rejestracji Zbiorów Danych Osobowych. W sprawach tych skierowano 6 pisemnych wezwań do przedstawienia dowodów wykonania obowiązków wynikających z tych decyzji. Z powodu braku odpowiedzi na ww. wezwania, powyższe sprawy zostały

przekazane do Zespołu do Spraw Egzekucji Administracyjnej. Ponadto Departament Rejestracji Zbiorów Danych Osobowych w 15 sprawach skierował wnioski o przekazanie decyzji administracyjnej do egzekucji administracyjnej. W wyniku powyższego dotychczas 7 zbiorów zostało ponownie zgłoszonych do rejestracji i wpisanych do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych ogólnokrajowego, jawnego rejestru danych osobowych.

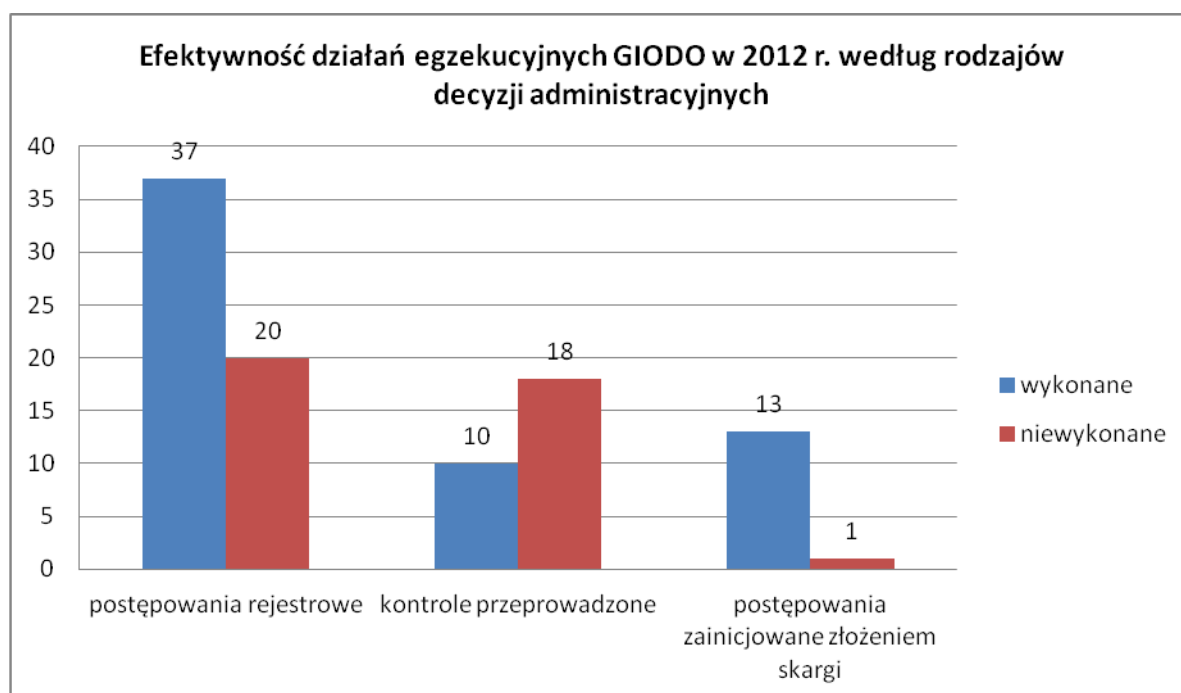
Podsumowując, w 2012 r. Generalny Inspektor wydał ogółem **99 decyzji administracyjnych zawierających nałożony na strony nakaz do wykonania i podlegających egzekucji administracyjnej**. Spośród wydanych decyzji **57** dotyczyło postępowań rejestrowych, **28** zostało wydanych w związku z przeprowadzonymi kontrolami, **14** wydano na skutek postępowania zainicjowanego skargą.



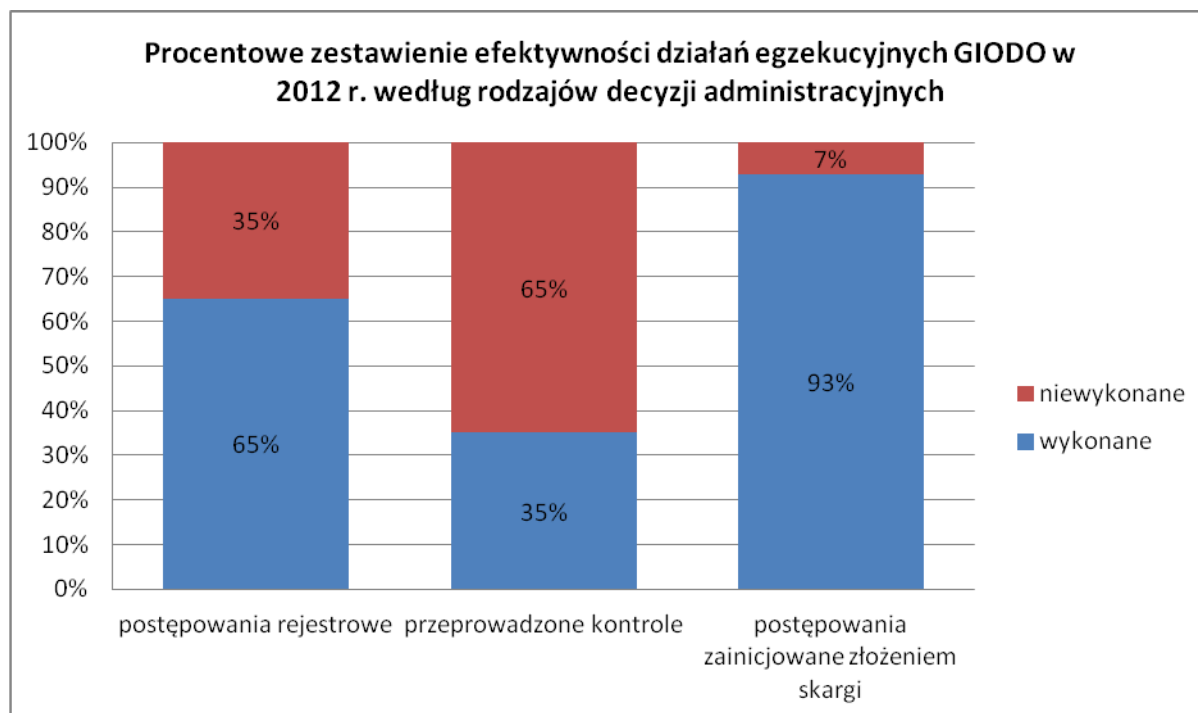
Wykres 25: *Liczbowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2012 r.*

Efektywność prowadzonych przez Generalnego Inspektora działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków, przedstawia się następująco: spośród 99 decyzji administracyjnych **wykonanych zostało przez zobowiązanych 60 decyzji**, zaś **39 decyzji na koniec 2012 r. pozostało niewykonanych**. Decyzje te zostały objęte działaniami egzekucyjnymi w 2013 r. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań Generalnego Inspektora oraz przeprowadzonych kontroli sprawdzających. Zobowiązani, którzy wykonali decyzję zrobili to w sposób dobrowolny, bez konieczności wystawiania tytułów wykonawczych i nakładania kary w postaci grzywny w celu przymuszenia. W jednym przypadku wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia zobowiązany wykonał w całości decyzję administracyjną Generalnego Inspektora.

Spośród decyzji wydanych w 2012 r. i wykonanych przez zobowiązanych w 2012 r. **37** dotyczyło postępowań rejestrowych, **10** zostało wydanych w związku z przeprowadzonymi kontrolami, **13** wydano na skutek postępowania zainicjowanego skargą. Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w 2012 r. wynosił **60%**. W odniesieniu do postępowań rejestrowych efektywność egzekucji wynosiła **65%**, wobec decyzji wydanych w związku z przeprowadzonymi kontrolami - **35%**, natomiast w stosunku do decyzji wydanych na skutek postępowań zainicjowanych skargą - **93%**.



Wykres 26: *Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GİODO w 2012 r.*



Wykres 27: *Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2012 r.*

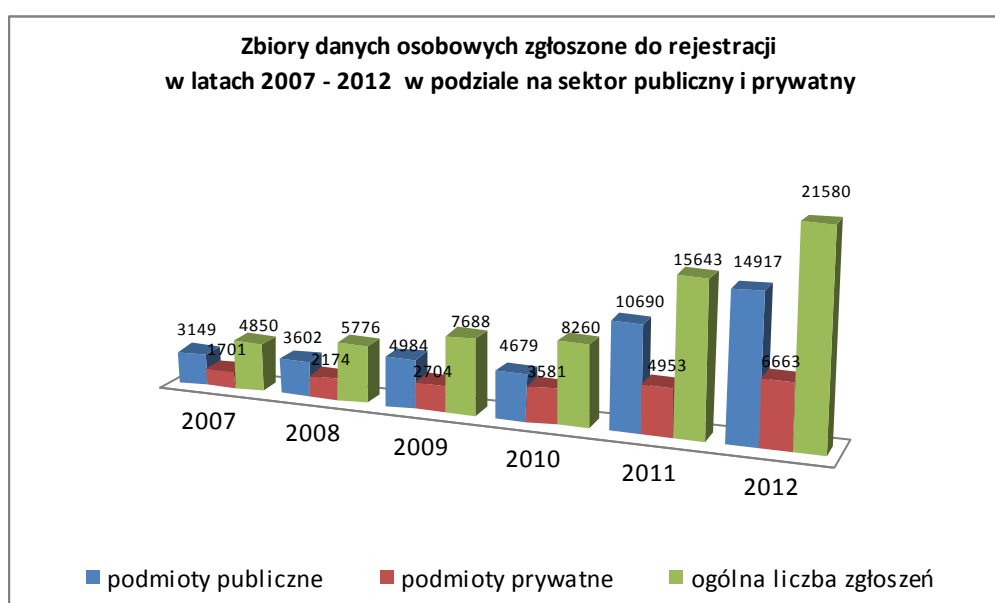
## 5. Prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach

Jednym z podstawowych zadań Generalnego Inspektora Ochrony Danych Osobowych jest prowadzenie ogólnokrajowego jawnego rejestru zbiorów danych osobowych. Z zadaniem tym skorelowany jest obowiązek zgłaszania zbiorów danych osobowych przez administratorów danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych<sup>129</sup>. Wskazane powyżej zadanie realizowane jest w Departamencie Rejestracji Zbiorów Danych Osobowych Biura GIODO. 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 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

<sup>129</sup> Zgodnie z art. 40 ustawy o ochronie danych osobowych, administrator danych obowiązany jest zgłosić zbiór danych do rejestracji, z wyjątkiem przypadków określonych w art. 43 ust. 1 ustawy.

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 2012, administratorzy danych wypełniając nałożony przepisami ustawy o ochronie danych osobowych obowiązek, zgłosili do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych **21580** zbiorów, z czego podmioty z sektora administracji publicznej zgłosiły **14917** zbiorów, co stanowi 68 % ogólnej liczby zgłoszeń dokonanych w tym okresie, zaś podmioty z sektora prywatnego 6663 zbiory, co stanowi 32 % ogólniej liczby zgłoszonych zbiorów.



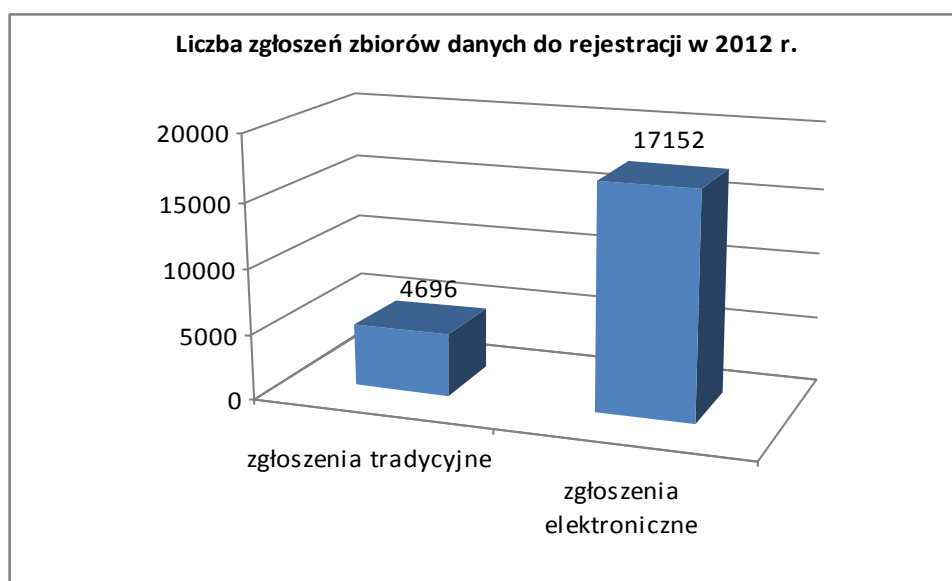
Wykres 28: *Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2007 - 2012.*

Analizując powyższy wykres należy wskazać, że w 2012 r. nastąpił wzrost o 6207 ogólnej liczby zgłoszeń nadesłanych do rejestracji (o 40 % więcej w stosunku do roku 2011, o 165 % w stosunku do roku 2010, zaś w odniesieniu do roku 2009 - aż o 184 %). Ten sam trend można zaobserwować w przypadku do zgłoszeń nadesłanych przez podmioty prywatne – w 2012 r. było ich o 1710 więcej w stosunku do roku poprzedniego (tj. o ok. 34 %).

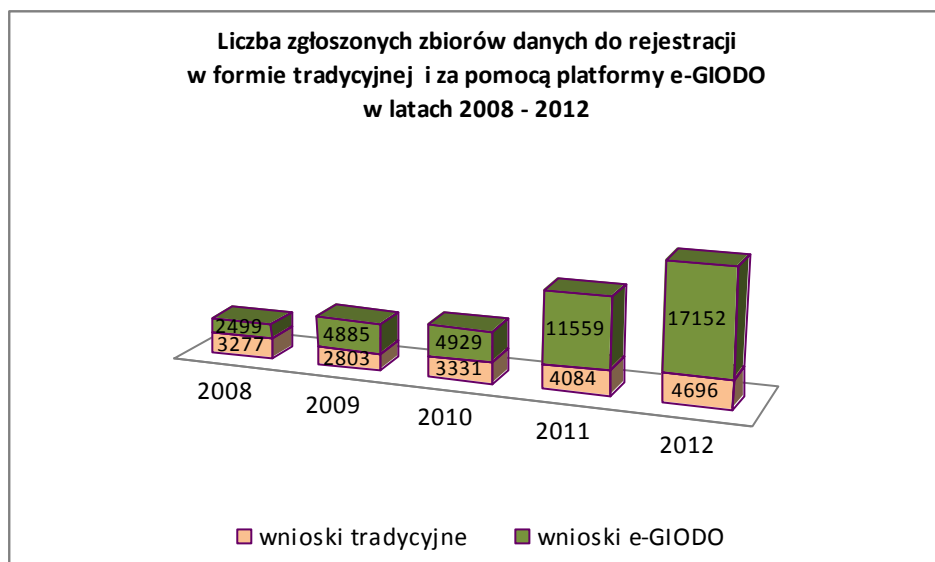
Znaczący wzrost liczby zgłoszeń wynikał przede wszystkim z rozwoju świadomości prawnej społeczeństwa w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych – w tym obowiązku rejestracji zbiorów danych osobowych - i miało związek z prowadzoną na szeroką skalę działalnością edukacyjną Generalnego Inspektora. Na taki stan rzeczy niewątpliwie wpływ miała także możliwość zgłaszania zbiorów drogą elektroniczną.

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” (e-GIODO).

W roku 2012 **przy użyciu programu wspomagającego** udostępnionego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych **zgłoszono do rejestracji 17 152 zbiory danych** osobowych, w tym 3579 zgłoszeń opatrzonych było podpisem elektronicznym, co stanowi 21 % wszystkich zgłoszeń przesłanych elektronicznie i 16 % ogólnej liczby zgłoszeń nadesłanych do rejestracji w 2012 r. Zgłoszenia dokonane drogą elektroniczną stanowiły 78 % wszystkich zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2012 r., co oznacza ich wzrost w stosunku do roku poprzedniego o 48 %.

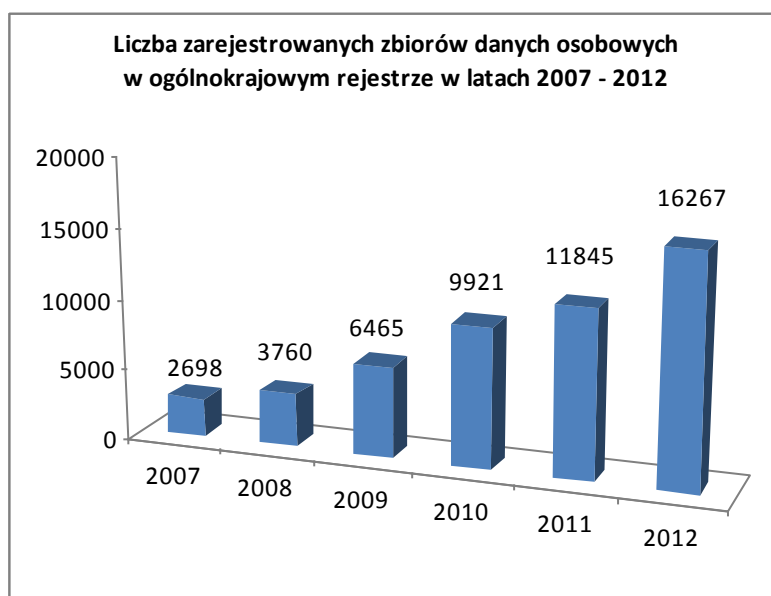


Wykres 29: **Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonanych w 2012 r. w formie tradycyjnej i elektronicznej.**



*Wykres 30: Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2008 - 2012 r. w formie tradycyjnej i przy użyciu elektronicznego programu wspomagającego, udostępnionego na stronie [www.giodo.gov.pl](http://www.giodo.gov.pl)*

W okresie sprawozdawczym do **ogólnokrajowego, jawnego rejestru zbiorów danych osobowych** prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych zostało **wpisanych 16267 zbiorów danych**, tj. o 37 % więcej niż w roku 2011 r., w którym było ich 11845.



*Wykres 31: Zestawienie porównawcze zarejestrowanych zbiorów danych osobowych w ogólnokrajowym rejestrze w latach 2007 - 2012.*

Chociaż liczba zarejestrowanych zbiorów danych osobowych stale rośnie, często informacje zawarte w zgłoszeniu nie pozwalają na zakończenie sprawy bez przeprowadzenia postępowania wyjaśniającego. Dzięki systemowi podpowiedzi w programie komputerowym służącym do realizacji

obowiązku rejestracji drogą elektroniczną, 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 ustawy<sup>130</sup>.

W 2012 roku w toku postępowań rejestracyjnych do wnioskodawców **skierowano 1390 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 skierowano do wnioskodawców, na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego, **1261 wezwań do uzupełnienia** w zgłoszeniu braku podpisu lub braku potwierdzenia umocowania wnioskodawcy do reprezentowania administratora danych.

W sytuacji, gdy brak było podstaw do zarejestrowania zgłoszonego zbioru danych, Generalny Inspektor Ochrony Danych Osobowych kierował do wnioskodawcy odpowiednie pismo.

W roku 2012 zostało wysłanych **670** takich pism, w tym **408 informujących administratorów danych o braku obowiązku rejestracji zbioru** wynikającym z przesłanek określonych w art. 43 ust. 1 ustawy oraz **262 pisma informujące o braku podstaw do dokonania wpisów w rejestrze** z innych przyczyn niż wynikające z powołanego powyżej przepisu (dotyczyły one zgłoszeń dokonanych przez

---

<sup>130</sup> Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych: 1) zawierających informacje niejawnie, 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 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.



podmioty niebędące 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).

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 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, na uwagę zasługuje przykład naruszenia zasady adekwatności, ujętej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Zasada ta oznacza, iż administrator danych przetwarzający dane osobowe jest w szczególności obowiązany zapewnić, aby dane te były adekwatne w stosunku do celów przetwarzania. Adekwatność (relevancja) powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi osobowymi a interesem administratora danych. Równowaga jest zachowana wówczas, gdy administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu ich przetwarzania. W przypadku administratorów z sektora prywatnego, istotnym zagadnieniem podlegającym ocenie w postępowaniu rejestracyjnym, w świetle powyższej zasady, było np. pozyskiwanie do prowadzonego zbioru numeru ewidencyjnego PESEL dla celów identyfikacji osób fizycznych.

Ustawa o ochronie danych osobowych w art. 6 ust. 1 stanowi, że za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zgodnie zaś z brzmieniem art. 6 ust. 2 ustawy, osobą możliwą do zidentyfikowania jest ta, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny. Takim numerem jest - zgodnie z art. 31a ust. 1 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (numer PESEL). Powołany przepis stanowi, że numer PESEL jest to 11-cyfrowy, stały symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne

cztery – to liczba porządkowa z oznaczeniem płci, a ostatnia jest cyfrą kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego. Numer ten, występując nawet bez zestawienia z innymi informacjami o osobie, jest daną osobową jednoznacznie identyfikującą osobę fizyczną. Organem właściwym do jego nadania jest minister właściwy do spraw wewnętrznych, zaś samo nadanie ma charakter czynności materialno-technicznej.

Z punktu widzenia ustawy o ochronie danych osobowych konieczne jest, aby administrator danych legitymował się jedną z przesłanek legalności przetwarzania danych osobowych. W odniesieniu do tzw. danych zwykłych zostały one wskazane w artykule 23 ust. 1 ustawy. Mają charakter równoprawny, zatem każda z nich może stanowić podstawę czyniącą proces przetwarzania danych zwykłych procesem legalnym. Określenie podstawy prawnej przetwarzania danych w zgłaszanym do rejestracji zbiorze jest obligatoryjnym obowiązkiem administratora wynikającym wprost z przepisów ustawy. Brak w zgłoszeniu informacji o podstawie prawnej gromadzenia danych stanowi przesłankę wydania przez Generalnego Inspektora decyzji o odmowie rejestracji zbioru danych.

Poniżej wskazane zostały przykłady pozyskiwania numeru ewidencyjnego PESEL dla celów identyfikacji osób fizycznych przez administratorów z sektora prywatnego, w odniesieniu do przesłanek legalizujących, zawartych w art. 23 ust. 1 ustawy:

- pozyskiwanie numeru PESEL w celu identyfikacji zwycięzców konkursu i loterii organizowanych przez administratora. Dodatkowo, w zależności od przedmiotu wygranej i jego wartości, numer PESEL laureatów był niezbędny w celu dopełnienia stosownych obowiązków względem organu podatkowego. Dane pozyskiwane były na podstawie zgody osoby, której dotyczą oraz w przypadku celów fiskalizacyjnych na podstawie ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2012 r. poz. 361);

- funkcjonowanie programu lojalnościowego/partnerskiego administratora. W przypadku tego typu zbiorów często zachodziła konieczność zbadania, czy przetwarzanie danych osobowych w nich gromadzonych nie naruszało zasady adekwatności (relewantności) wyrażonej w przepisach ustawy o ochronie danych osobowych. Naruszenie tej zasady stanowi bowiem przesłankę wydania decyzji o odmowie rejestracji. Administratorzy danych dokonując zgłoszeń zbiorów danych prowadzonych w związku z realizacją programów lojalnościowych/partnerskich, bardzo często w treści zgłoszeń informowali o pozyskiwaniu do zbiorów między innymi numeru ewidencyjnego PESEL. Przetwarzanie tej danej w powyższych zbiorach mogło naruszać zasadę adekwatności. Należy jednak wskazać, że w określonych sytuacjach jej przetwarzanie było dopuszczalne w związku z realizacją programów lojalnościowych/partnerskich, gdy na przykład uczestnikowi programu przyznana została nagroda rzeczowa lub finansowa i – co za tym idzie - konieczność jej rozliczenia w urzędzie skarbowym.

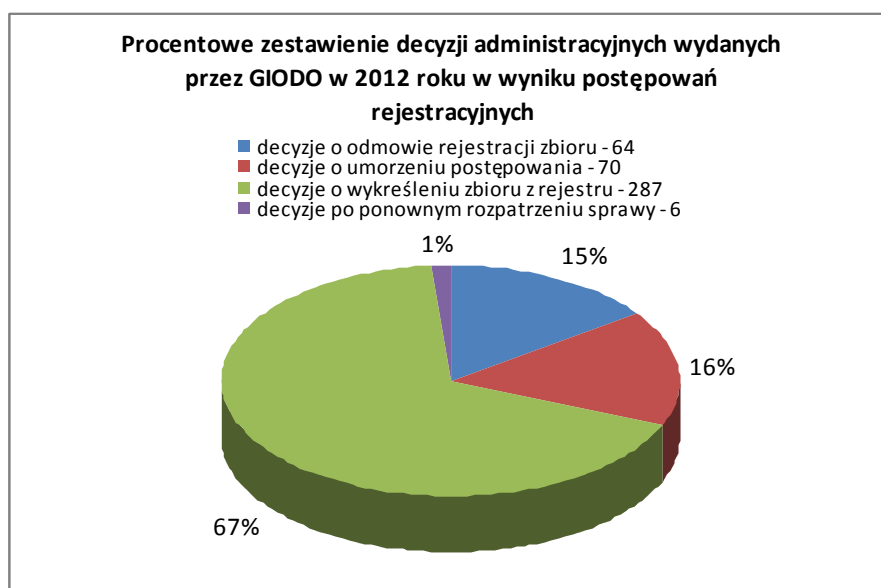
Podstawą prawną gromadzenia danych była zgoda osoby, której one dotyczą oraz przepisy ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (Dz. U. z 2012 r. poz. 361);

- przetwarzanie przez usługodawcę świadczącego usługi drogą elektroniczną m.in. numeru ewidencyjnego PESEL usługobiorcy, który był niezbędny do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi, na podstawie art. 18 ust. 1 pkt 2 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.);
- prowadzenie rejestracji gości w ośrodkach gier, co stanowiło warunek wstępu do lokalu. Osoba kierująca ośrodkiem gier albo upoważniony przez nią pracownik, sprawdzał tożsamość gościa na podstawie dokumentu potwierdzającego jego wiek i tożsamość. Rejestracja obejmowała sprawdzenie i zapisanie w rejestrze gości daty i godziny wejścia konkretnej osoby do ośrodka gier oraz jego danych osobowych, obejmujących m.in. numer PESEL, na podstawie art. 15a ust. 1-3 ustawy z dnia 19 listopada 2009 r. o grach hazardowych (Dz. U. z 2009 r. Nr 201, poz. 1540 z późn. zm.);
- prowadzenie ewidencji wypłaconych (wydanych) wygranych przez podmiot zarządzający gry hazardowe, których wartość wynosiła co najmniej 20.000 zł. W ewidencji umieszczane były m.in. dane osoby wygrywającej w postaci numeru PESEL, na podstawie art. 20 ust. 7 pkt 1 ustawy z dnia 19 listopada 2009 r. o grach hazardowych (Dz. U. z 2009 r. Nr 201, poz. 1540 z późn. zm.);
- przetwarzanie numeru ewidencyjnego PESEL użytkownika przez dostawcę publicznie dostępnych usług telekomunikacyjnych, który był uprawniony do przetwarzania tego numeru w związku ze świadczoną użytkownikowi usługą, na podstawie art. 161 ust. 2 pkt 5 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.);
- identyfikacja osób uczestniczących w meczu piłki nożnej przez organizatora imprezy (osobę prawną, osobę fizyczną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, przeprowadzającą imprezę masową). Zakres przetwarzanych danych identyfikujących osoby uczestniczące w meczu piłki nożnej obejmował m.in. numer PESEL na podstawie art. 13 ust. 1 i 4 ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (Dz. U. Nr 62, poz. 504 z późn. zm.);
- wymiana informacji pomiędzy wydawcami elektronicznych instrumentów płatniczych na temat posiadaczy nienależycie wykonujących umowy o elektroniczny instrument płatniczy. W przypadku posiadaczy będących osobami fizycznymi informacje obejmowały m.in. numer PESEL, na podstawie art. 68 ust. 1 i 2 ustawy z dnia 12 września 2012 r. o elektronicznych instrumentach płatniczych (Dz. U. Nr 169, poz. 1385 z późn. zm.);
- żądanie podania pracodawcy (jednostka organizacyjna, choćby nie posiadała osobowości prawnej, a także osobie fizycznej, jeżeli zatrudniają one pracowników) - poza danymi dotyczącymi imienia (imion) i nazwiska, imion rodziców, daty urodzenia, miejsca zamieszkania, wykształcenia oraz

przebiegu dotychczasowego wykształcenia - także numeru PESEL, na podstawie art. 22<sup>1</sup> § 2 pkt 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.);

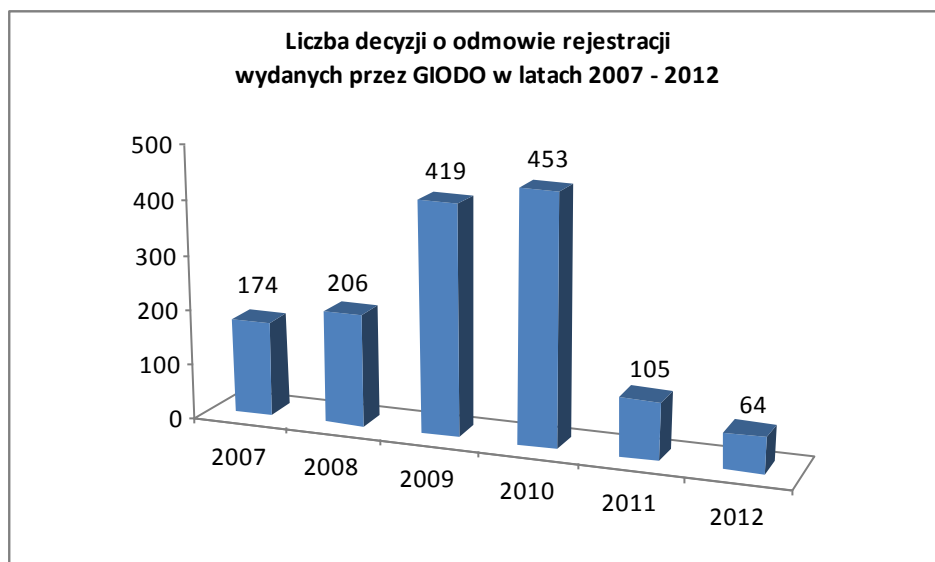
- przetwarzanie numeru ewidencyjnego PESEL było uzasadnione w celu realizacji umowy, gdy osoba, której dane dotyczą, była jej stroną lub gdy było to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, a także w celu dochodzenia roszczeń w przypadku niewykonania bądź nienależytego wykonania umowy (art. 23 ust. 1 pkt 3 i 5 ustawy o ochronie danych osobowych).

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał ogółem **427 decyzji administracyjnych w związku z postępowaniem rejestracyjnym**. Spośród nich **64 decyzje dotyczyły odmowy rejestracji zbioru danych, 70 - umorzenia postępowania, 287 decyzji dotyczyło wykreślenia zbioru danych z ogólnokrajowego jawnego rejestru zbiorów danych osobowych, zaś 6 decyzji wydano po ponownym rozpatrzeniu sprawy.**



Wykres 32: *Procentowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2012 r.*

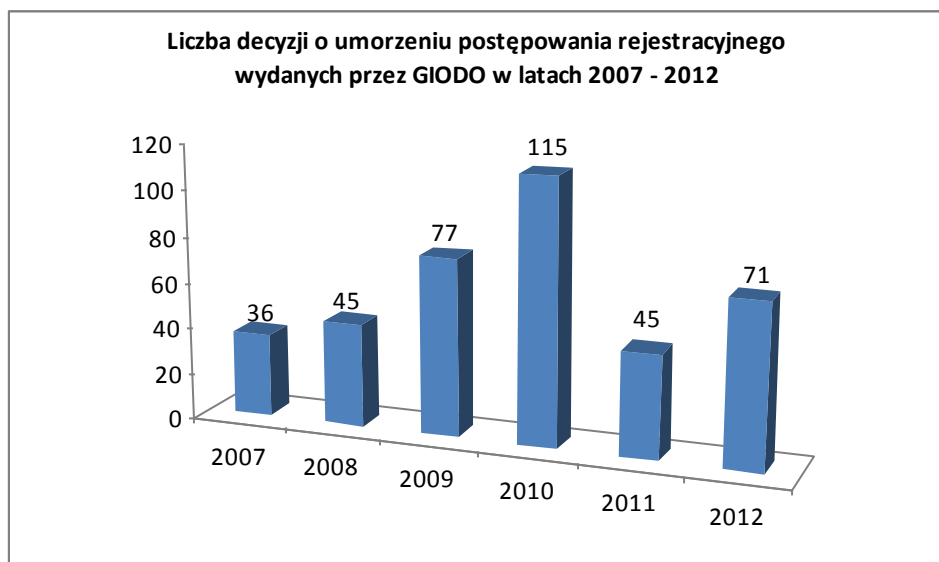
Działania legislacyjne, edukacyjne, organizacyjne i techniczne podjęte w ostatnich latach przez Generalnego Inspektora Ochrony Danych Osobowych, miały znaczny wpływ na zmniejszenie się liczby **decyzji o odmowie rejestracji zbioru danych**, przy jednoczesnym wzroście liczby zbiorów zarejestrowanych.



Wykres 33: *Zestawienie porównawcze liczby decyzji o odmowie rejestracji zbioru wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007 – 2012.*

Jak już o tym była mowa, w wyniku nowelizacji ustawy o ochronie danych osobowych, która weszła w życie 7 marca 2011 r., na Generalnego Inspektora Ochrony Danych Osobowych zostało nałożone nowe zadanie, polegające na zapewnieniu wykonania przez zobowiązanych obowiązków wynikających z decyzji GODO przez stosowanie środków egzekucyjnych. W roku 2012 r. po przeprowadzeniu postępowań wszczętych nie wcześniej niż dnia 7 marca 2011 r., Generalny Inspektor Ochrony Danych Osobowych wydał **57 decyzji zawierających nakazy wynikające z art. 44 ust. 2 ustawy o ochronie danych osobowych.**

Zgodnie z art. 44 ust. 4 ustawy o ochronie danych osobowych, administrator danych może ponownie zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych po usunięciu wad, które były powodem odmowy rejestracji tego zbioru. W tym trybie zostało zgłoszonych do rejestracji 21 zbiorów. Natomiast w 6 sprawach, w których Generalny Inspektor Ochrony Danych Osobowych wydał decyzję o odmowie rejestracji, brak było podstaw do stwierdzenia niewykonania decyzji – administratorzy informowali, w szczególności, iż nie rozpoczęli gromadzenia danych osobowych w przedmiotowym zbiorze lub też zaprzestali przetwarzania danych w zgłoszonym do rejestracji zbiorze.



**Wykres 34: Zestawienie porównawcze liczby decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007 - 2012.**

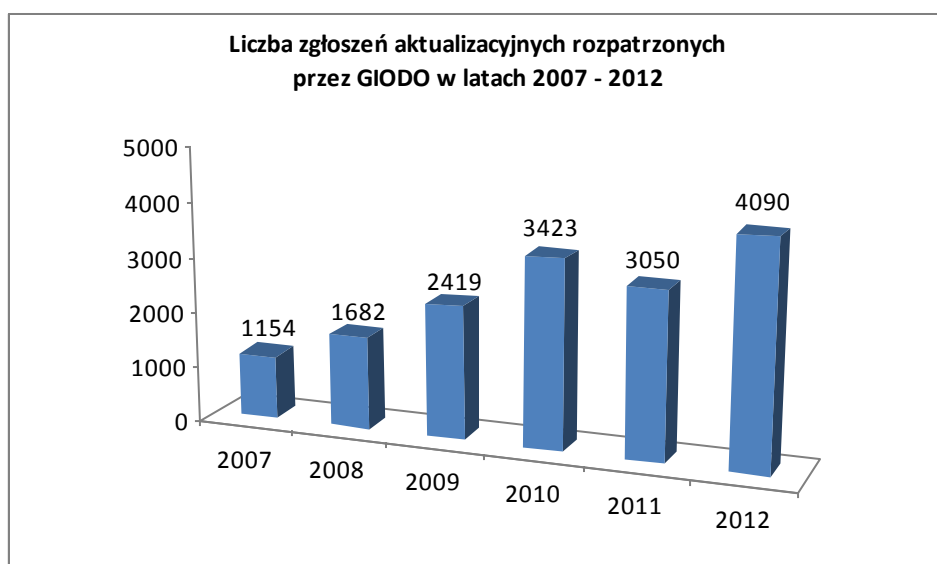
Należy zwrócić uwagę, że wraz z odmową rejestracji zbioru Generalny Inspektor nakazuje ograniczenie przetwarzania danych wyłącznie do ich przechowywania lub zastosowanie innych środków, określonych w art. 18 ustawy, np. usunięcie uchybień, zastosowanie dodatkowych środków zabezpieczających zgromadzone 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 wymagania przewidziane w ustawie o ochronie danych osobowych.

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, z jednej strony, nałożony na administratorów obowiązek zgłaszania Generalnemu Inspektorowi Ochrony Danych Osobowych każdej zmiany informacji, o których mowa w art. 41 ust. 1 ustawy<sup>131</sup>, zaś z drugiej strony, instytucja wykreślenia zbioru, dające możliwość porządkowania rejestru, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych<sup>132</sup>.

<sup>131</sup> Zgodnie art. 41 ust. 2 ustawy o ochronie danych osobowych, administrator danych obowiązany jest zgłaszać każdą zmianę informacji zawartych w zgłoszeniu rejestracyjnym w terminie 30 dni od dnia dokonania zmiany w zbiorze danych.

<sup>132</sup> Wykreślenie z rejestru zbiorów danych osobowych jest dokonywane w drodze decyzji administracyjnej, jeżeli zaprzestano przetwarzania danych w zarejestrowanym zbiorze lub gdy rejestracji dokonano z naruszeniem prawa (Art. 44a ustawy).

W 2012 roku **rozpatrzonych zostało 4090 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<sup>133</sup>.

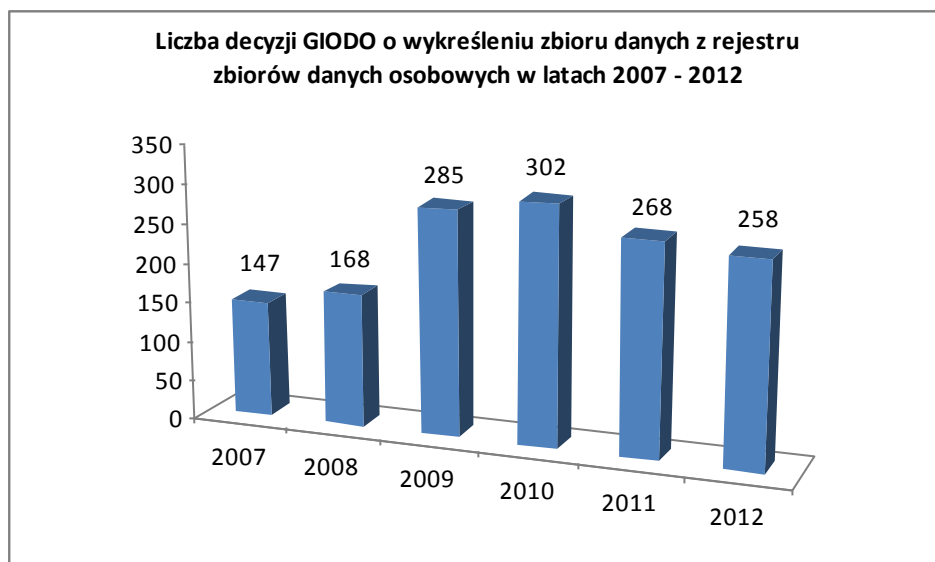


Wykres 35: *Zestawienie porównawcze liczby zgłoszeń aktualizacyjnych rozpatrzonych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007 - 2012.*

Generalny Inspektor Ochrony Danych Osobowych wydał **258 decyzji o wykreśleniu** zbioru danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych z powodu zaprzestania przetwarzania danych w zbiorze.

---

<sup>133</sup> W wyniku wejścia w życie w dniu 7 marca 2011 r. nowelizacji ustawy o ochronie danych osobowych, nastąpiło sprecyzowanie terminu, w jakim administrator powinien zgłosić GIODO zmianę informacji o zakresie przetwarzanych danych, dotyczącą rozszerzenia tego zakresu o tzw. dane szczególnie chronione, o których mowa w art. 27 ust. 1 ustawy. Zgodnie z dodanym przepisem ust. 3 w art. 41 ustawy, administrator zobowiązany jest dokonać ww. zgłoszenia przed dokonaniem zmiany w zbiorze.



*Wykres 36: Zestawienie porównawcze liczby decyzji o wykreśleniu zbioru danych z rejestru, wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007 - 2012.*

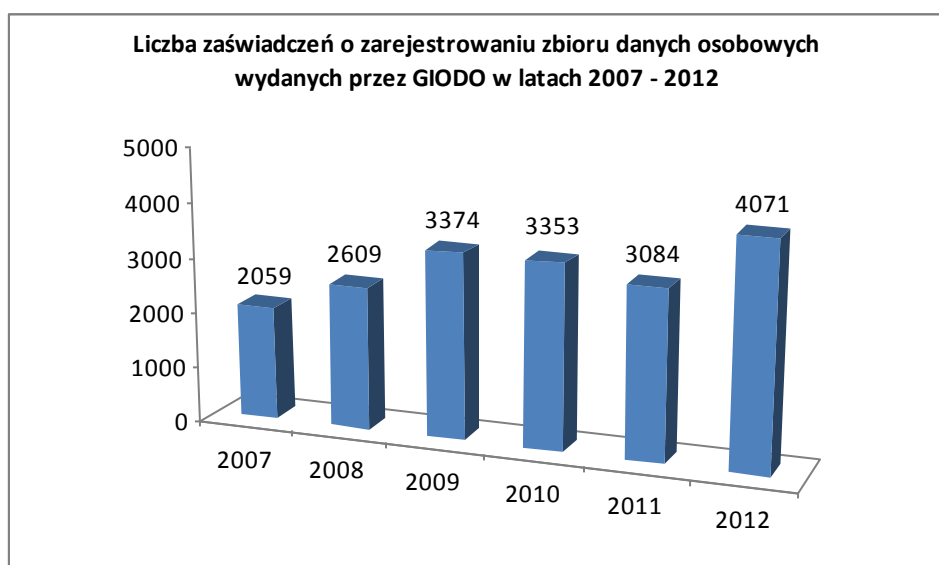
Zadaniem Generalnego Inspektora Ochrony Danych Osobowych jest także udzielanie informacji o zarejestrowanych zbiorach, w szczególności wydawanie zaświadczeń o zarejestrowaniu zbioru danych osobowych. W omawianym okresie Generalny Inspektor Ochrony Danych Osobowych wydał **4071 zaświadczeń o zarejestrowaniu zbioru**. Generalny Inspektor wydaje zaświadczenia o zarejestrowaniu zgłoszonego zbioru danych na wniosek administratora<sup>134</sup>. Jednakże w przypadku zarejestrowania zbioru danych, w którym przetwarzane są dane osobowe szczególnie chronione określone w art. 27 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wydaje zaświadczenie z urzędu, niezwłocznie po dokonaniu rejestracji takiego zbioru<sup>135</sup>.

---

<sup>134</sup> Art. 42 ust. 3 ustawy

<sup>135</sup> Art. 42 ust. 4 ustawy o ochronie danych osobowych.

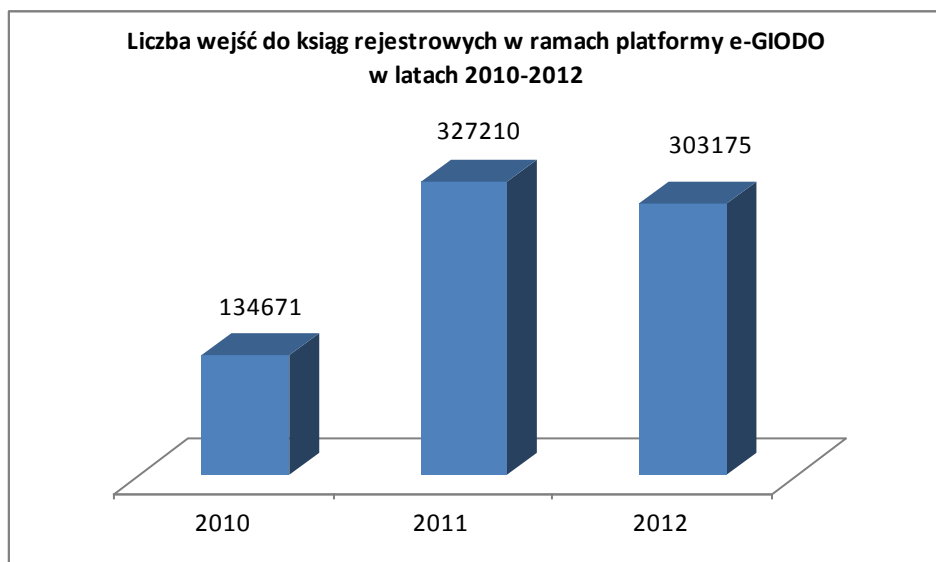




Wykres 37: *Zestawienie liczby zaświadczeń o zarejestrowaniu zbioru danych osobowych wydanych przez Generalnego Inspektora Ochrony Danych osobowych w latach 2007 - 2012.*

Celem rejestracji jest także upublicznienie informacji o zbiorach zarejestrowanych w ogólnokrajowym jawnym rejestrze zbiorów danych osobowych. Każda osoba, korzystając z prawa do przeglądania rejestru, może uzyskać ogólne informacje o administratorach danych i prowadzonych przez nich zbiorach danych osobowych. 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. Informacje zawarte w rejestrze udostępniane są na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych ([www.giodo.gov.pl](http://www.giodo.gov.pl)) w ramach elektronicznej 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 2012 w elektronicznej wersji rejestru odnotowano **303175** wejść do poszczególnych ksiąg rejestrowych i liczba ta jest porównywalna z stosunku do poprzedniego roku sprawozdawczego.

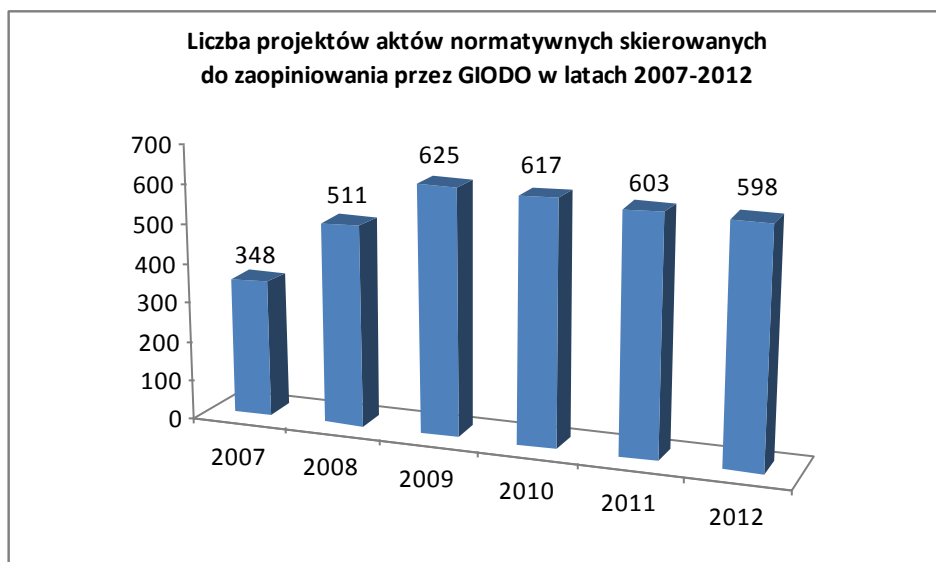


Wykres 38: *Liczbowe zestawienie wejść do poszczególnych ksiąg rejestrowych w rejestrze zbiorów danych osobowych w ramach platformy e-GIODO w latach 2010 - 2012.*

## 6. 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 przez ustawodawcę 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 2012 do Biura GIODO wpłynęło do zaopiniowania **598 projektów aktów prawnych**. W 2009 r. wpłynęło 625 projektów, w 2010 r. – 617, w 2011 r. – 603, natomiast w 2012 – 598. Od czterech lat można więc zauważyć niewielki, ale systematyczny spadek w tej kategorii, co ilustruje poniższy wykres.



Wykres 39: *Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2007-2012.*

Uczestnicząc w pracach legislacyjnych na szczeblu europejskim, w związku z przyjęciem przez Komisję Europejską w dniu 25 stycznia 2012 r. pakietu zmian regulacji UE w zakresie ochrony danych, w tym wniosku dotyczącego *rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (tzw. ogólne rozporządzenie o ochronie danych)*, Generalny Inspektor Ochrony Danych Osobowych przedstawił swoje stanowisko do ww. aktu. Projekt ten jest niezwykle istotny z punktu widzenia organizacji ochrony danych osobowych w państwach członkowskich Unii Europejskiej z uwagi na jego bezpośrednią stosowalność i przyświecający mu cel, jakim jest harmonizacja prawa materialnego w tym zakresie.

W ramach uwag ogólnych do projektu, w pierwszej kolejności za jego pozytywną cechę, zwłaszcza biorąc pod uwagę trudną sytuację budżetową, Generalny Inspektor Ochrony Danych Osobowych uznał fakt, że prawodawca unijny wprost wskazał na konieczność zapewnienia przez państwo członkowskie niezależnemu organowi nadzorczemu odpowiednich zasobów ludzkich, technicznych i finansowych dla realizacji jego, istotnie rozszerzonych w projekcie ogólnego rozporządzenia, zadań (art. 47 ust. 5 i ust. 7 projektu ogólnego rozporządzenia). W kontekście prowadzonych dyskusji nad sposobem wypełniania przez poszczególne podmioty obowiązków wynikających z przepisów prawa europejskiego, szczególnie cenna wydaje się, zawarta w art. 47 ww. projektu, konstatacja, że posiadanie odpowiednich zasobów ludzkich, technicznych, finansowych i infrastrukturalnych (w tym odrębnego budżetu) stanowi jeden z warunków niezależności organu nadzorczego.

Organ do spraw ochrony danych osobowych wskazał ponadto na prawidłową i zasługującą na poparcie ideę, która legła u podstaw opiniowanego projektu. Zgodnie z nią system ochrony danych

osobowych powinien opierać się nie na formalnych obowiązkach, lecz na odpowiedzialności (w tym finansowej) administratorów danych, z szerokim uwzględnieniem koncepcji *privacy by design* (art. 33 i art. 34 projektu rozporządzenia o ochronie danych) oraz *privacy by default* (m.in. art. 30 ww. projektu).

Jednocześnie jednak w projekcie zostały dostrzeżone liczne przepisy budzące wątpliwości. Przyjęta w art. 8 ust. 1 projektu ogólnego rozporządzenia konstrukcja prawna, w myśl której, w odniesieniu do usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgoda rodzica (opiekuna) na przetwarzanie danych dziecka jest wymagana tylko w odniesieniu do dzieci poniżej 13 roku życia, pozostaje w sprzeczności z przepisami księgi pierwszej części ogólnej tytułu II działu I rozdziału I ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.). Skoro po zmianie ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), wprowadzonej przez art. 1 pkt 1 ustawy z dnia 29 października 2010 roku o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz. 1497), nie budzi już żadnych wątpliwości, że skutkiem oświadczenia woli jakim jest zgoda na przetwarzanie danych osobowych (art. 7 pkt 5 ustawy o ochronie danych osobowych), jest rozporządzenie w określonym zakresie dobrem osobistym (prawem do prywatności) osoby składającej takie oświadczenie, to ocena zdolności do złożenia przedmiotowego oświadczenia musi się odbywać w oparciu o wyżej powołane przepisy ustawy – Kodeks cywilny. Nie może zaś umknąć uwadze, że art. 11 ustawy – Kodeks cywilny przyznaje pełną zdolność do czynności prawnych jedynie osobom pełnoletnim (w rozumieniu art. 10 tej ustawy), zaś ważność czynności prawnej jednostronnej, mocą której osoba ograniczona w zdolności do czynności prawnych (czyli w wieku od 13 lat do pełnoletności, nieubezwłasnowolniona całkowicie – art. 15 ustawy – Kodeks cywilny) rozporządza swoim prawem, kodeks ten uzależnia od zgody jej przedstawiciela ustawowego (art. 19 w zw. z art. 17 ustawy – Kodeks cywilny). Tym samym – w świetle obowiązującego prawa polskiego – niedopuszczalne byłoby samodzielne wyrażenie przez dziecko w wieku od lat 13 zgody na przetwarzanie jego danych osobowych.

Po drugie, organ do spraw ochrony danych osobowych stwierdził, że zawarta w projekcie rozporządzenia o ochronie danych definicja zgody nie wydaje się do końca zbieżna z poglądami Grupy Roboczej Art. 29 (GR Art. 29) dotyczącymi tej problematyki. Stanowisko to wyrażone zostało m.in. w Opinii 15/2011 GR Art. 29 w sprawie definicji zgody, przyjętej w dniu 13 lipca 2012 r. Niezależny europejski organ doradczy w zakresie ochrony danych i prywatności przedstawił w niej dogłębną analizę pojęcia zgody stosowanego w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31). Niemniej jednak wydaje się w pełni zasadne uwzględnienie tejże opinii w rozważaniach na temat instytucji

zgody toczących w ramach prac nad tworzeniem nowych europejskich przepisów o ochronie danych osobowych, w których – pojawiając się w rozmaitych kontekstach (art. 6, 8, 9, 17, 20, 44, 83, 18 projektu ogólnego rozporządzenia o ochronie danych) – odgrywa ona niezwykle istotną rolę. Grupa Robocza Art. 29 stwierdziła we ww. opinii, iż: (...) *nie jest ona przekonana, że przyszłe ramy prawne powinny wymagać wyrażnej zgody co do zasady dla wszystkich rodzajów operacji przetwarzania danych, w tym obecnie objętych art. 7 dyrektywy. Uważa, że jednoznaczna zgoda, która obejmuje wyraźną zgodę, ale także zgodę wynikającą z jednoznacznego działania, powinna pozostać obowiązującą normą. Wybór ten daje większą elastyczność dla administratorów danych do zbierania zgód i cała procedura może być przez to szybsza i bardziej przyjazna dla użytkownika*". Projektodawca europejski poprzez tak sformułowaną definicję czyni wyrażenie zgody w sposób wyraźny warunkiem jej ważności. Jednocześnie w preambule podkreśla znaczenie tego kryterium, odnosząc się jedynie do zgody na przetwarzanie danych wrażliwych: (...) *Dane te nie powinny być przetwarzane, chyba że podmiot danych wyraźnie wyrazi na to zgodę*" (motyw 41).

Uwaga została również zwrócona w kierunku nie najbardziej trafnego przetłumaczenia sformułowania „main establishment”, które w oficjalnym tłumaczeniu pojawia się jako „główna siedziba”, choć bardziej poprawne wydawałoby się jego przełożenie na „główny zakład”. Pojęcie to jest istotne zwłaszcza przy określaniu kwestii tak zasadniczej, jak terytorialny zakres zastosowania przepisów rozporządzenia (art. 3 ust. 2 i 3 projektu ogólnego rozporządzenia o ochronie danych). Za szczególną ostrożnością przy interpretacji tego pojęcia przemawia zwłaszcza okoliczność, iż „główna siedziba” – za oficjalnym tłumaczeniem na język polski – rozumiana jest inaczej niż wynika to z przepisów ustawy – Kodeks cywilny, który za siedzibę uważa miejscowość, w której ma siedzibę organ zarządzający osoby prawnej, jeśli ustawa lub oparty na niej statut nie stanowi inaczej. Podczas gdy z siedzibą w rozumieniu projektu ogólnego rozporządzenia utożsamiana jest lokalizacja, gdzie podejmowane są najważniejsze decyzje dotyczące celów, warunków i sposobów przetwarzania danych, jeśli zaś decyzji dotyczących tych aspektów nie podejmuje się w Unii, za główną siedzibę uważa się miejsce, w którym odbywa się główna działalność w zakresie przetwarzania w kontekście działalności zakładu administratora w Unii; jeśli zaś chodzi o podmiot przetwarzający, „główna siedziba” oznacza miejsce, w którym znajduje się jego zarząd w Unii. Prawidłowe określenie miejsca uznawanego za siedzibę zyskuje również istotne znaczenie w przypadku ustalania właściwego organu nadzorczego, gdy przetwarzanie danych osobowych odbywa się w kontekście działalności administratora lub podmiotu przetwarzającego ustanowionych na terytorium Unii, a administrator lub podmiot przetwarzający prowadzą działalność w więcej niż jednym państwie członkowskim – wówczas bowiem nadzór nad działalnością administratora lub podmiotu przetwarzającego jest sprawowany przez organ nadzorczy głównej siedziby tego administratora lub podmiotu przetwarzającego (tzw. one-stop-shop). Powyższe oznacza, iż przy ustalaniu głównej siedziby podmiotu przesądzającego o zakresie terytorialnym

zastosowania przepisów ogólnego rozporządzenia o ochronie danych lub właściwości organu nadzorczego, należy brać pod uwagę wymienione w tej definicji kryteria, nie kierując się rozumieniem tego pojęcia z prawa cywilnego czy prawa spółek handlowych, co może prowadzić do pewnych wątpliwości odnośnie wykładni tego pojęcia.

W wątpliwość poddana została również zaproponowana w analizowanym projekcie koncepcja profilowania osób fizycznych (art. 20). Obawę wzbudza po pierwsze definicja środków opartych na profilowaniu (art. 20 ust. 1 projektu), zgodnie z którą są to środki, które m.in. wywołują skutki prawne dotyczące tej osoby fizycznej. Takie ujęcie sugeruje niebezpieczne zawężenie stosowania regulacji dotyczących profilowania – przyznających osobom fizycznym, co do zasady, prawo niepodlegania środkom na nim opartych – do sytuacji, gdy wpływ środków na nim opartych jest wywierany w sferze praw i obowiązków osób. Projektodawca unijny zostawia co prawda pewien margines, w ramach którego za środki oparte na profilowaniu mogą zostać uznane środki inne niż wywołujące skutki prawne, wskazując w dalszej kolejności, iż są nimi także środki mające istotny wpływ. Jednakże wysoce wątpliwe jest, czy przy tak nieostro sformułowanym kryterium – sugerującym szerokie możliwości zróżnicowanej wykładni – zakresem regulacji zostaną objęte znaczące przypadki stosowania mechanizmu profilowania, istotne w potocznym rozumieniu (jak np. dobieranie konkretnych przekazów reklamowych). Powyższe skłania do postawienia pytania, czy nacisk na skutki prawne wywołane profilowaniem stanowić powinien istotę regulacji mającej odpowiednio identyfikować to zjawisko i stwarzać odpowiednie gwarancje ochrony przed jego swobodnym rozprzestrzenianiem się.

W odniesieniu do treści art.17 projektu dotyczącego prawa do bycia zapomnianym i do usunięcia danych, organ do spraw ochrony danych osobowych stwierdził, że konieczne jest rozważenie znaczenia tego przepisu z punktu widzenia ochrony praw podmiotu danych, zwłaszcza, gdy mowa o przetwarzaniu danych w środowisku internetowym, które z natury umożliwia dokonywanie nieskończenie wielu różnych operacji na raz wprowadzonych danych, w związku z czym realizacja ww. praw mogłaby nastręczać pewne trudności techniczne. Ponadto nałożenie na administratora danych – w przypadku, gdy podaje on dane osobowe do wiadomości publicznej i w odniesieniu do danych, za których publikację odpowiada – obowiązku poinformowania osób trzecich przetwarzających takie dane, że podmiot danych wnioskuje o usunięcie linków do danych, kopii lub replikacji tych danych osobowych, może doprowadzić do sytuacji zgoła odwrotnej, tj. do przypomnienia o konkretnym podmiocie danych podmiotom, które incydentalnie i w związku z jednorazową potrzebą te dane pozyskały. Paradoksalnie zatem możliwy byłby scenariusz, że owe „osoby trzecie” – których na domiar projektodawca nie definiuje – nie przetwarzają już danych osobowych podmiotu danych lub otrzymały jego odrębny sprzeciw wobec przetwarzania dotyczących go danych. W związku z tym powstaje pytanie o celowość takiego informowania, które służyć przecież

powinno ochronie praw podmiotu danych. Dodatkowo nie jest jasne, jak projektodawca unijny – wobec braku mechanizmu egzekwowania działania od osób trzecich – widzi możliwość efektywnej realizacji praw podmiotu danych. Podobne zastrzeżenia dotyczyły art. 13 projektu ogólnego rozporządzenia, który nakłada na administratora danych wymóg poinformowania każdego odbiorcy, któremu ujawniono dane, o wszelkich operacjach ich poprawienia lub usunięcia dokonanych zgodnie z art. 16 i 17, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Przy okazji tej uwagi Generalny Inspektor podkreślił, że kwestie o zasadniczym znaczeniu z punktu widzenia realizacji prawa do bycia zapomnianym i do usunięcia danych przez podmiot danych, tj. kryteria i wymogi w poszczególnych sektorach oraz w szczególnych sytuacjach przetwarzania danych czy też warunki usuwania linków do danych kopii lub replikacji danych osobowych z publicznie dostępnych usług łączności, o których mowa w ust. 2, zostały przekazane Komisji Europejskiej do uregulowania w formie aktów delegowanych, zgodnie z art. 86. Bez znajomości całości przepisów składających się na ww. prawa nie sposób jest w pełni odnieść się do tej problematyki.

Zaniepokojenie wzbudziła ponadto konstrukcja prawna – zaproponowana w art. 20 ust. 2 lit. a niniejszego projektu, jako pierwszy wyjątek od generalnego zakazu profilowania – przewidująca wyłączenie obowiązku pozyskiwania zgody osoby, której dane dotyczą, gdy przetwarzanie dotyczących jej danych osobowych odbywa się w trakcie zawierania umowy lub wykonania umowy, jeśli wniosek w sprawie zawarcia lub wykonania umowy złożony przez podmiot danych został zrealizowany lub jeśli przewidziano właściwe środki zabezpieczenia słusznym interesów podmiotu danych, jak np. prawo do uzyskania interwencji ze strony człowieka. Powołanie się na tak ujęte odstępstwo od generalnego zakazu profilowania, wiążące się ze zjawiskami powszechnie występującymi w obrocie gospodarczym, wydaje się stosunkowo łatwe i co więcej, lżejsze gatunkowo od przewidzianych w dalszej kolejności w art. 20 ust. 2 wyjątków, zgodnie z którymi profilowanie jest dopuszczalne, gdy jest to wyrażnie dozwolone przez prawo Unii lub państwa członkowskiego, które ustanawia również właściwe środki w celu zabezpieczenia słusznym interesów podmiotu danych (art. 20 ust. 2 lit. b projektu rozporządzenia o ochronie danych) lub odbywa się na podstawie zgody podmiotu danych, z zastrzeżeniem warunków określonych w art. 7 oraz właściwych gwarancji (art. 20 ust. 2 lit. c projektu). Nie kwestionując zasadności przyjmowania instrumentów służących przedstawianiu przez przedsiębiorców ofert produktów czy usług w większym stopniu dopasowanych do konsumentów, nie można jednak tracić z pola widzenia, że projektowany akt prawny ma służyć także ochronie podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych. Powyższe zmusza zatem do poddania w wątpliwość, czy tak ukształtowany wyjątek rzeczywiście zapewni podmiotom danych efektywną ochronę przed niepożądanym, czy też nie do końca uświadamianym profilowaniem.

Akceptując samą koncepcję nałożenia na administratorów danych w art. 31 – 32 projektu obowiązku zgłaszania niezależnemu organowi nadzorczemu (w Rzeczypospolitej Polskiej – Generalnemu Inspektorowi Ochrony Danych Osobowych) naruszenia ochrony danych osobowych – w znaczeniu nadanemu temu pojęciu przez art. 4 pkt 9 omawianego projektu - organ do spraw ochrony danych osobowych zwrócił uwagę na fakt, że wskazany w art. 31 ust. 1 omawianego aktu prawnego termin dokonania takiego zgłoszenia (24 godziny) jest odmienny od – przewidzianego w projektowanym (art. 1 pkt 127 projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw – wersja z dnia 12.02.2012 r.) art. 174 a ust. 1 ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.) – terminu na zgłaszanie naruszeń danych osobowych w sektorze telekomunikacyjnym (3 dni). Prowadzić to może w przyszłości do zaistnienia wątpliwości odnośnie wzajemnego stosunku tych przepisów i niejasności, w jakim terminie (dwudziestoczworgodzinny czy trzydniowy) dostawca publicznie dostępnych usług telekomunikacyjnych ma dopełnić obowiązku powiadomienia Generalnego Inspektora Ochrony Danych Osobowych o naruszeniu ochrony danych osobowych.

Odnosząc się do zagadnień szczegółowych w analizowanym projekcie, Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę na fakt, że kwestia przekazania – mocą jego przepisów – Komisji Europejskiej do uregulowania w formie aktów delegowanych szeregu zagadnień, powinna być przedmiotem odrębnych, pogłębionych rozważań. Abstrahując od okoliczności, że zakres zagadnień przekazanych do unormowania w aktach delegowanych jest zbyt szeroki, nie może umknąć uwadze, że już na etapie prac dotyczących projektu ogólnego rozporządzenia o ochronie danych, projekty tych aktów delegowanych powinny zostać przedstawione do analizy i wszechstronnej dyskusji. Bez znajomości ich treści trudno bowiem w opinii Generalnego Inspektora Ochrony Danych Osobowych wyrazić ostateczne stanowisko.

Warto także dodać, że trwają prace nad *Dyrektywą Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych.*

W stanowisku GIODO wobec analizowanego projektu dyrektywy podkreślenia wymaga, iż projekt ten zawiera liczne gwarancje ochrony i realizacji praw osób, których dane będą przetwarzane, zaś w sytuacjach, gdy realizacja tych praw przez podmiot danych mogłaby zaszkodzić uzasadnionemu interesowi publicznemu (np. utrudniać dochodzenia, negatywnie wpływać na zapobieganie przestępstwom oraz wykrywanie ich sprawców, godzić w bezpieczeństwo publiczne, itp.), statuuje prawo podmiotu danych do wystąpienia do niezależnego organu nadzorczego o dokonanie niezbędnego sprawdzenia zgodności z prawem procesu przetwarzania (art. 14 projektu). O wprowadzenie rozwiązania polegającego na umożliwieniu organowi do spraw ochrony danych osobowych jedynie



poinformowania osoby, której dane dotyczą, że dokonał stosownego zbadania dotyczącego tej osoby procesu przetwarzania danych i ewentualnie podjął niezbędne działania, Generalny Inspektor Ochrony Danych Osobowych wnosił już podczas prac odnoszących się do projektu ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej.

Jeśli dodać do zakresu kompetencji organu nadzorczego, iż projekt dyrektywy w art. 28 – 29 przewiduje wprowadzenie procedury zgłaszania do organu nadzorczego przypadków naruszenia ochrony danych osobowych (w znaczeniu nadanemu temu pojęciu przez art. 3 pkt 9 projektu), to nie ulega wątpliwości, że – w przypadku objęcia przez Generalnego Inspektora Ochrony Danych Osobowych funkcji organu nadzorczego w rozumieniu tych przepisów – Biuro Generalnego Inspektora Ochrony Danych Osobowych wymagać będzie istotnego wzmocnienia kadrowego i finansowego. Problem ten został dostrzeżony przez autorów projektu dyrektywy, którzy w art. 40 ust. 5 tego projektu uznali posiadanie przez organ nadzorczy odpowiednich zasobów ludzkich, technicznych, finansowych, lokalowych i infrastrukturalnych za gwarancję rzeczywistej niezależności takiego organu.

W okresie objętym sprawozdaniem Generalny Inspektor opiniował *Założenia projektu ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych*<sup>136</sup>. Pozytywnie ustosunkował się do kierunku zmian, w którym podąża projektodawca, będącego zbieżnym w dużej mierze z opinią Europejskiego Inspektora Ochrony Danych z dnia 18 kwietnia 2011 r. na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego dotyczącego dyrektywy w sprawie zatrzymywania danych (2011/C279/01), a także Opinią Grupy Roboczej Art. 29 nr 3/2006 w sprawie dyrektywy Parlamentu Europejskiego i Rady 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE, przyjętej przez Radę w dniu 21 lutego 2006 r. (Dz. U. L 105 z 13.4.2006, str. 54). Na forum europejskim toczą się obecnie prace nad jej nowelizacją. Po przygotowaniu raportu z przeprowadzonej procedury oceny wpływu, Komisja Europejska zamierzała przedstawić nową propozycję jeszcze w 2012 roku.

Przechodząc do uwag o charakterze szczegółowym, organ do spraw ochrony danych osobowych jako pozytywną ocenił propozycję powołania w strukturach podmiotów uprawnionych do pozyskiwania i wykorzystania danych retencyjnych, instytucji pełnomocnika ds. ochrony danych osobowych, postrzegając ją jako próbę działania mającego na celu przełożenie na grunt nowotworzonych przepisów rozwiązań, które funkcjonują już pod rządami obecnie obowiązujących regulacji. Takie rozwiązania przyjęte w przepisach szczególnych funkcjonują na gruncie art. 22b ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2006 r. Nr 104, poz.

---

<sup>136</sup> DOLiS-033-278/12

708 z późn. zm.) w CBA (pełnomocnik do spraw kontroli przetwarzania przez CBA danych osobowych). Osoba sprawująca tę funkcję nadzoruje zgodność przetwarzania danych osobowych gromadzonych przez CBA z przepisami ustawy oraz przepisami o ochronie danych osobowych (art. 22b ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym). Abstrahując od faktu istnienia tego typu szczególnego rozwiązania w ustawie regulującej działalność jednej ze służb specjalnych w Polsce, która podlega specyficznemu reżimowi, organ do spraw ochrony danych osobowych wskazał na istnienie konstrukcji wprowadzonej w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zobowiązującej administratora danych – w przypadku, gdy on sam nie wykonuje czynności nadzorczych – do wyznaczenia osoby, której zadaniem jest nadzorowanie przestrzegania zasad ochrony danych, tj. administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy o ochronie danych osobowych). Propozycja powołania pełnomocnika ds. ochrony danych osobowych nie byłaby zatem rozwiązaniem o zupełnie nowej jakości. Jednocześnie Generalny Inspektor Ochrony Danych Osobowych zauważył, że istnienie tego typu funkcji w CBA, a w przyszłości w innych służbach, rozwiązuje jedynie problem kontroli wewnętrznej, do której zapewniania administratorzy danych są już zobowiązani przepisami ustawy o ochronie danych osobowych. Zaniepokojenie organu do spraw osobowych budził natomiast brak odniesienia się w przedłożonym do zaopiniowania projekcie założeń, do kwestii kontroli zewnętrznej prowadzonej przez niezależny organ, mimo iż jej uregulowania należałoby oczekiwać w związku zapowiedziami przedstawionymi w opracowanym w 2011 r. „Raporcie dotyczącym retencji danych telekomunikacyjnych. Propozycje wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych”. Przedmiotowy raport podkreślał ograniczone możliwości takiej kontroli wobec służb specjalnych realizujących swoje kompetencje w zakresie wykonywania czynności operacyjno – rozpoznawczych i jako remedium proponował model niezależnego, powoływanego przez parlament organu kontrolnego, którego celem byłaby kontrola przestrzegania przez służby specjalne Konstytucji Rzeczypospolitej Polskiej oraz innych przepisów prawa, szczególnie w zakresie praw i wolności obywatelskich. Model ten funkcjonuje w niektórych krajach, jak Belgia, Kanada, Holandia, Norwegia i Szwecja. W dokumencie tym dość kompleksowo odniesiono się do przedmiotowej instytucji, omawiając tak istotne z punktu widzenia jej działania zagadnienia, jak powoływanie i skład, zadania, kompetencje oraz wyniki pracy organu kontrolnego. Tym bardziej zatem nieobecność regulacji dotyczących kontroli wewnętrznej w materiale będącym przedmiotem analizy budziło zdziwienie.

W projekcie założeń zaproponowano, aby dane telekomunikacyjne mogły być pozyskiwane i wykorzystywane przez uprawnione służby, prokuraturę i sądy dla potrzeb postępowań w sprawie ścigania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej

3 lata oraz postępowań o ściganie przestępstw popełnionych przy użyciu środków komunikacji elektronicznej, za wyjątkiem przestępstw celnych. Tymczasem dyrektywa 2006/24/WE, określając swój cel stanowi, iż jest nim zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw określonych w ustawodawstwie każdego państwa członkowskiego (art. 1 ust. 1 dyrektywy nr 2006/24/WE). W świetle takiego ujęcia kategorii przestępstw, w walce z którymi pomocna miałyby być retencja danych telekomunikacyjnych przez usługodawców, wydaje się, że za „poważne przestępstwa” na gruncie prawa polskiego należy uznać zbrodnie, tj. zgodnie z art. 7 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.) czyny zagrożone karą pozbawienia wolności na czas nie krótszy od lat 3 albo karą surowszą. Ustawodawca tymczasem w projekcie założeń, zaliczając do grupy „poważnych przestępstw” nie tylko te sankcjonowane karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, ale również inne kategorie przestępstw, wprowadza tym samym zupełnie nową konstrukcję prawną. Skoro zatem przepisy Kodeksu karnego w wyczerpujący sposób określają, jak należy interpretować pojęcie „poważnego przestępstwa” (używanego przez ustawodawcę unijnego), to propozycję przewidującą odrębną jego wykładnię, należałoby ocenić jako nieuzasadnioną.

Generalny Inspektor Ochrony Danych Osobowych odniósł się także do – wymagającej jego zdaniem doprecyzowania – koncepcji wprowadzenia w ustawach określających kompetencje organów i służb uprawnionych do pozyskiwania i wykorzystywania danych telekomunikacyjnych (niezawierających jeszcze takich regulacji), obowiązku niszczenia danych zbędnych w postępowaniu. W opinii organu do spraw ochrony danych osobowych w przypadku jakichkolwiek rejestrów konstrukcja prawna dotycząca niszczenia danych powinna zakładać, że dane – co do zasady – podlegają zniszczeniu, gdy są już zbędne, a wyjątki od tej zasady – przewidujące zachowanie danych, które mogą okazać się w pewnych sytuacjach potrzebne – powinny być wyraźnie wskazane w ustawie w formie zamkniętej listy, analogicznie, jak ma to miejsce w przypadku kontroli operacyjnej. Pozwoliłoby to uniknąć – występującego w praktyce – problemu przechowywania danych nawet wtedy, kiedy nie są one już niezbędne.

Ponadto Generalny Inspektor Ochrony Danych Osobowych wskazał, że projektodawca nie odpowiedział w analizowanych założeniach na pytanie, czy osoby, których dane były przetwarzane przez organy państwa, mają być informowane o tym fakcie po zakończeniu postępowania. Przesądzenie o tym zagadnieniu wydaje się zasadne również z uwagi na fakt, iż jest ono często podnoszone – jako budzące wątpliwości – w dyskusjach na forach organizacji pozarządowych. Nie negując zastrzeżeń policji czy też służb specjalnych co do informowania osób, wobec których w danym

momencie nie pozyskano żadnych istotnych dowodów dla prowadzonego przeciwko nim postępowania, szczególnie w przypadku rozpracowywania zorganizowanych grup przestępczości, to należy jednak skonstatować, iż w akcie prawnym wprowadzającym zmiany do obowiązujących ustaw w celu kompleksowego podejścia do problematyki pozyskiwania i wykorzystywania danych telekomunikacyjnych i mającym stanowić odpowiedź na problemy wyłaniające się w praktyce stosowania przepisów czy też w związku ze zmieniającym się otoczeniem – wskazane byłoby jednoznaczne uregulowanie tej kwestii.

Kolejna szczególnie istotna opinia Generalnego Inspektora dotyczyła **Projektu założeń projektu ustawy o redukcji niektórych obciążeń administracyjnych w gospodarce**<sup>137</sup>. Nadmienić należy, że w trakcie prac legislacyjnych Rada Ministrów zdecydowała o przeniesieniu tego projektu do kolejnej transzy deregulacji i oddzielnym wniesieniu go do Sejmu, a następnie o zmianie nazwy tego dokumentu na „Projekt założeń projektu ustawy o ułatwieniu warunków działalności gospodarczych”. Propozycje zmian ustawy o ochronie danych osobowych, które miałyby być wprowadzone w związku z projektem deregulacji gospodarki, zostały przedstawione we wcześniejszym piśmie Generalnego Inspektora Ochrony Danych Osobowych z dnia 29 maja 2012 r. Generalny Inspektor wskazał, że przedłożony mu do zaopiniowania – dokument „**Projekt założeń projektu ustawy o redukcji niektórych obciążeń administracyjnych w gospodarce**” zawierał co prawda propozycje zmian ustawy o ochronie danych osobowych zasługujące zasadniczo na akceptację, niemniej jednak propozycje te odbiegają od tych, zawartych we ww. piśmie z 29 maja 2012 roku. Co więcej, niektóre z rozwiązań zamieszczonych w projekcie założeń Generalny Inspektor uznał za zbyt daleko idące i pozostające w sprzeczności z przepisami prawa europejskiego, normującymi kompetencje niezależnego organu do spraw ochrony danych osobowych. Wskazał, że w odniesieniu do postulatu wyłączenia – przewidzianego w rozdziale 6 ustawy o ochronie danych osobowych – obowiązku rejestracji zbiorów danych osobowych wobec administratorów danych, którzy powołali i zgłosili do Generalnego Inspektora Ochrony Danych Osobowych administratora bezpieczeństwa informacji (pkt 2.30 projektu założeń), to może on zyskać poparcie organu do spraw ochrony danych osobowych, jeśli w projekcie założeń zamieszczone zostaną stosowne rozwiązania uzupełniające. Generalny Inspektor zaznaczył bowiem, że przepisy ustawy o ochronie danych osobowych dotyczące obowiązku rejestracji zbiorów danych stanowią implementację unormowań zamieszczonych w rozdziale II sekcji IX dyrektywy 95/46/WE który reguluje instytucję tzw. "notyfikacji" (zawiadomienia), tj. nałożonego na administratora danych obowiązku powiadamiania organu nadzorczego o zamierzonych operacjach przetwarzania danych. Nadmienił, że w świetle regulacji ww. dyrektywy 95/46/WE niedopuszczalne jest zrezygnowanie przez państwo członkowskie z obowiązku notyfikacji (zawiadomienia), ale możliwe

---

<sup>137</sup> DOLiS-033-306/12/43304

jest jego uproszczenie bądź zwolnienie z tego wymogu w wypadkach wskazanych w art. 18 ust. 2 tego aktu prawnego. Przedmiotowy przepis dopuszcza m.in., aby państwa członkowskie uprościły obowiązek notyfikacyjny lub z niego zwolniły, jeżeli administrator danych wyznaczy urzędnika ds. ochrony danych osobowych (data protection official), który będzie odpowiedzialny za 1) zapewnienie w sposób niezależny wewnętrznego (u administratora danych) stosowania krajowych przepisów o ochronie danych osobowych (opartych na dyrektywie 95/46/WE) oraz 2) prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych, zawierającego takie same elementy jak rejestr ogólnokrajowy, prowadzony przez niezależny organ do spraw ochrony danych osobowych. Generalny Inspektor wskazał, że ustawodawca polski nie skorzystał dotychczas z możliwości uregulowania – przewidzianej w dyrektywie 95/46/WE – instytucji urzędnika ds. ochrony danych osobowych. Wymieniony w art. 36 ust. 3 polskiej ustawy o ochronie danych osobowych administrator bezpieczeństwa informacji (ABI) nie spełnia bowiem warunków do uznania go za urzędnika ds. ochrony danych osobowych w rozumieniu dyrektywy 95/46/WE. W opinii Generalnego Inspektora ustawa nie gwarantuje mu bowiem niezależności oraz zbyt wąsko określa jego zadania w stosunku do uregulowań ww. dyrektywy. Ze względu na opisane wyżej wymogi prawa unijnego kompleksowe zwolnienie z obowiązku rejestracyjnego administratora danych, który powołał i zgłosił – celem przeprowadzenia rejestracji – do Generalnego Inspektora Ochrony Danych Osobowych administratora bezpieczeństwa informacji (ABI), wymaga jednocześnie zmiany przepisu ustawy o ochronie danych osobowych odnoszącego się do zadań administratora bezpieczeństwa informacji i uregulowania jego usytuowania organizacyjnego w jednostce administratora danych. Generalny Inspektor wyjaśnił, że podstawowym zadaniem ABI w jednostce organizacyjnej, oprócz prowadzenia jawnego rejestru zbiorów danych, winno być zapewnienie stosowania przepisów o ochronie danych osobowych, w szczególności poprzez:

- przeprowadzanie czynności polegających na sprawdzeniu zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych (kontrola wewnętrzna);
- zapewnienie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy o ochronie danych osobowych, oraz nadzorowanie przestrzegania zasad w niej określonych;
- zaznajamianie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zauważył przy tym, że wprowadzenie nowych przepisów dotyczących statusu i zadań ABI zapewni zachowanie podstawowych standardów wyznaczonych dyrektywą 95/46/WE, jak niezależność w wykonywaniu zadań, obowiązek zapewnienia stosowania w jednostce organizacyjnej przepisów o ochronie danych osobowych, w szczególności poprzez przyznanie kompetencji do kontroli wewnętrznej w zakresie przestrzegania tych przepisów oraz prowadzenie wewnętrznego rejestru

zbiorów danych.

Zdaniem Generalnego Inspektora niezbędne było także zamieszczenie w ustawie o ochronie danych osobowych – co jest już postulowane w projekcie założeń – rozwiązań określających status ABI, na który składają się: wymogi stawiane osobie mającej pełnić omawianą funkcję (pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych, wykształcenie wyższe, legitymowanie się odpowiednią wiedzą z zakresu przepisów o ochronie danych osobowych, niekaralność za przestępstwo popełnione z winy umyślnej), organizacyjne usytuowanie funkcji ABI w jednostce administratora danych (bezpośrednia podległość kierownikowi jednostki organizacyjnej, który zapewnia niezbędne środki i organizacyjną odrębność administratora bezpieczeństwa informacji w niezależnym wykonywaniu przez niego zadań) oraz dopuszczenie nałożenia na ABI innych zadań, niż określone w ustawie o ochronie danych osobowych (pod warunkiem, że nie naruszają one możliwości prawidłowego wykonywania zadań wyznaczonych w ustawie).

Zasadnym z punktu widzenia Generalnego Inspektora było także wprowadzenie możliwości powoływania zastępców ABI. Generalny Inspektor nadmienił, że w piśmie z dnia 29 maja 2012 r. sugerował możliwość powołania ABI przez administratora danych (a więc dobrowolność), wiążąc jednocześnie z faktem powołania ABI u danego administratora danych, możliwość zwolnienia tego administratora z pewnych obowiązków wynikających z ustawy o ochronie danych osobowych. Z drugiej strony Generalny Inspektor stanął na stanowisku, że w znowelizowanych przepisach ustawy o ochronie danych osobowych powinien znaleźć się zapis, że w przypadku niepowołania ABI, na administratorze danych ciążyć będzie obowiązek wykonywania nadzoru wewnętrznego nad bezpieczeństwem przetwarzania danych w jednostce organizacyjnej. Jeśli chodzi o propozycję wyłączenia obowiązku rejestracji zbiorów danych prowadzonych przez administratorów danych w sposób tradycyjny, tj. bez wykorzystywania systemów informatycznych, to Generalny Inspektor zwrócił uwagę na treść art. 18 ust. 5 dyrektywy 95/46/WE, zgodnie z którym państwa członkowskie mogą postanowić, że niektóre lub wszystkie nieautomatyzowane operacje przetwarzania danych osobowych będą zgłaszane lub ustalać dla takich operacji uproszczony tryb zawiadamiania. Zdaniem Generalnego Inspektora cytowany – *a contrario* – przepis może być interpretowany w ten sposób, że państwa członkowskie mają pewną swobodę w kwestii objęcia operacji przetwarzania danych w zbiorach tradycyjnych obowiązkiem rejestracji. Zaznaczył przy tym, że taka wykładnia postanowień art. 18 ust. 5 dyrektywy 95/46/WE nie jest powszechnie przyjęta w państwach członkowskich Unii Europejskiej. W tym stanie rzeczy Generalny Inspektor zaakceptował tę propozycję z uwzględnieniem, że zwolnienie z obowiązku rejestracyjnego nie może znaleźć zastosowania w odniesieniu do zbiorów danych zawierających dane szczególnie chronione w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych (zastrzeżenie takie słusznie znalazło się w pkt 2.30 projektu założeń). Nie wzbudziła zaś zastrzeżeń Generalnego Inspektora propozycja nałożenia na administratorów danych

obowiązku powiadamiania Generalnego Inspektora o powołaniu albo odwołaniu administratora bezpieczeństwa informacji (ABI) oraz zobligowania organu do spraw ochrony danych osobowych do prowadzenia rejestru administratorów bezpieczeństwa informacji (pkt 2.31 *in principio* projektu założeń). Nie ulega wątpliwości, iż w toku prac legislacyjnych koncepcja ta musi przyjąć formę całościowej regulacji obejmującej: zasady dokonywania zgłoszeń, zakres informacji zawartych w zgłoszeniach, zasady prowadzenia przez Generalnego Inspektora przedmiotowego rejestru, formę prawną rozstrzygnięć organu do spraw ochrony danych osobowych związanych z rejestracją i skutki prawne tej rejestracji. Generalny Inspektor przypominał też, że w piśmie z dnia 29 maja 2012 roku przedłożył propozycję brzmienia wskazanych wyżej unormowań:

- rozszerzenie kompetencji rejestracyjnych Generalnego Inspektora Ochrony Danych Osobowych miałyby zostać wprowadzone poprzez zmianę obecnego art. 12 ustawy o ochronie danych osobowych;

- obowiązek zgłoszenia dotyczyłby: faktu powołania oraz odwołania ABI oraz zmian danych objętych zgłoszeniem; administrator danych miałby informować Generalnego Inspektora Ochrony Danych Osobowych o fakcie powołania/odwołania ABI oraz o zmianie danych objętych zgłoszeniem w terminie 14 dni od dnia powołania (odwołania, zmiany);

- określenie w ustawie o ochronie danych osobowych zakresu informacji zawartych w zgłoszeniu oraz w ogólnokrajowym jawnym rejestrze administratorów bezpieczeństwa informacji, jak również możliwości wydawania zaświadczeń o zarejestrowaniu ABI;

- wprowadzenie przepisów regulujących wykreślenie ABI z rejestru w drodze czynności materialno-technicznej (w przypadku powiadomienia przez administratora danych o odwołaniu ABI) oraz na podstawie wydawanej z urzędu decyzji administracyjnej podlegającej natychmiastowemu wykonaniu (jeżeli administrator danych nie powiadomił o odwołaniu ABI, administrator bezpieczeństwa informacji nie spełnia ustawowych warunków jego powołania lub nie wykonuje swoich ustawowych zadań);

- dodanie przepisu regulującego skutki wykreślenia dla administratora danych (brak możliwości skorzystania ze zwolnienia z obowiązku rejestracji zbiorów w związku z powołaniem ABI);

- wprowadzenia regulacji przyznającej administratorowi danych możliwość ponownego zgłoszenia do rejestracji ABI wykreślonego z rejestru oraz zobowiązującej Generalnego Inspektora Ochrony Danych Osobowych, w przypadku stwierdzeniu wyeliminowania przyczyn wykreślenia, do wydania decyzji administracyjnej w przedmiocie wpisu ABI do rejestru lub decyzji administracyjnej odmawiającej wpisu do rejestru, jeżeli nie zostały usunięte przyczyny wykreślenia z rejestru.

Generalny Inspektor negatywnie zaś ocenił postulowane (pkt 2.31 *in fine* projektu założeń) rozwiązanie, zgodnie z którym w przypadku – wykonywanej na wniosek Generalnego Inspektora Ochrony Danych Osobowych przez administratora bezpieczeństwa informacji – „uproszczonej kontroli przestrzegania przepisów o ochronie danych osobowych”, następowałoby wyłączenie – przewidzianej

w art. 12 pkt 1 ustawy o ochronie danych osobowych – bezpośredniej kontroli Generalnego Inspektora Ochrony Danych Osobowych w zakresie zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Uznał bowiem, że rozwiązanie takie jest niezgodne z przepisami prawa europejskiego, a w szczególności z art. 28 ust. 1 i 3 dyrektywy 95/46/WE, jak również naruszające – proklamowaną w prawie europejskim – zasadę niezależności organu do spraw ochrony danych osobowych (zob. np. wyrok Trybunału Sprawiedliwości UE w sprawie C-518/07) i dlatego zdaniem Generalnego Inspektora winno być one wykreślone z projektu założeń. Przypomniawszy również, iż – zgodnie z art. 28 ust. 1 dyrektywy 95/46/WE – każde państwo członkowskie zapewni, że jeden lub więcej organów władzy publicznej będzie odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów przyjętych przez państwa członkowskie na mocy niniejszej dyrektywy. Stosownie zaś do dyspozycji art. 28 ust. 3 ww. dyrektywy, każdy organ nadzorczy jest w szczególności wyposażony w uprawnienia dochodzeniowe, jak np. prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych. W polskim porządku prawnym, w myśl art. 8 ust. 1 ustawy o ochronie danych osobowych, takim organem nadzorczym jest Generalny Inspektor Ochrony Danych Osobowych, któremu przepisy ustawy o ochronie danych osobowych nie tyle przyznają uprawnienie, lecz wręcz nakładają obowiązek sprawowania kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych (art. 12 pkt 1 ustawy o ochronie danych osobowych). Zwrócił też uwagę, że również w przepisach – przedstawionego dnia 25 stycznia 2012 roku – projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), które ma zastąpić dyrektywę 95/46/WE, zostało podkreślone uprawnienie do przeprowadzenia kontroli przysługujące każdemu organowi nadzorczemu. W ocenie Generalnego Inspektora zaproponowane zatem w pkt 2.31 *in fine* projektu założeń rozwiązanie nie tylko narusza obowiązujące przepisy dyrektywy 95/46/WE, ale jest także niezgodne z tendencjami w zakresie regulacji ochrony danych osobowych w prawie unijnym. Wyraźnie przy tym zaznaczył, że prawo Unii Europejskiej nie zna możliwości wyzbycia się przez organy nadzorcze uprawnień kontrolnych na rzecz urzędników ds. ochrony danych osobowych nawet wtedy, gdy mechanizm nadzoru jest tworzony na potrzeby jednej instytucji (jak ma to miejsce w przypadku Europejskiego Biura Policji). Dodał również, że – w związku z wprowadzoną w projekcie założeń „uproszczoną kontrolą przestrzegania przepisów o ochronie danych osobowych” – w ustawie o ochronie danych osobowych należałoby dodać przepis nakładający na administratora bezpieczeństwa informacji obowiązek sporządzenia – po przeprowadzonej kontroli wewnętrznej – sprawozdania zawierającego informacje określone w ustawie. Sprawozdanie to byłoby przedkładane Generalnemu Inspektorowi Ochrony Danych Osobowych. Wobec pozostałych rozwiązań zamieszczonych w projekcie założeń Generalny Inspektor zgłosił następujące zastrzeżenia. W związku



z propozycją (pkt 3.6 projektu założeń) publikowania wszystkich wyroków sądów powszechnych na stronach Biuletynu Informacji Publicznej, Generalny Inspektor zasugerował daleko idącą ostrożność przy przyjmowaniu tego rozwiązania. Nie negując – słusznie podnoszonej przez projektodawcę – zasady jawności i transparentności działania sądów zauważył jednak, że niekiedy publikacja orzeczenia wraz z uzasadnieniem skutkować może niedającymi się naprawić negatywnymi konsekwencjami dla uczestników postępowania sądowego (w tym pokrzywdzonych). Samo usunięcie z treści orzeczenia podstawowych danych osobowych (imię, nazwisko, adres) może – w określonym stanie faktycznym – nie zapewnić rzeczywistej niemożliwości identyfikacji osób biorących udział w postępowaniu i narazić te osoby na stygmatyzację w środowisku, w którym przebywają. Dlatego też – w przypadku podtrzymywania przez projektodawcę jego propozycji z pkt 3.6 projektu założeń – Generalny Inspektor Ochrony Danych Osobowych wniósł o określenie katalogu spraw, w których publikacja wyroków na stronach Biuletynu Informacji Publicznej nie będzie dopuszczalna.

Generalny Inspektor pozytywnie zaś ocenił (zamieszczony w pkt 1.8 projektu założeń) postulat skrócenia do 3 dni roboczych terminu przekazywania przez banki do Biura Informacji Kredytowej S.A. informacji o wszystkich ratach spłaconych przez klientów tych banków. Podzielając w pełni argumenty zawarte w uzasadnieniu tej propozycji zasugerował również jej uzupełnienie poprzez stosowne skrócenie (np. również do 3 dni roboczych) – wskazanego w uzasadnieniu – trzydziestodniowego terminu na uaktualnienie danych w zbiorze danych prowadzonym przez Biuro Informacji Kredytowej S.A. po otrzymaniu przez ten podmiot raportu aktualizacyjnego z banku. Przy okazji zwrócił uwagę, że autor projektu założeń nie wskazał w pkt 1.8 przepisu prawa, który będzie podlegał zmianie w przypadku przyjęcia tej propozycji. W uzupełnieniu przedstawionego wyżej stanowiska wobec projektu założeń zwrócił się także o uwzględnienie w tym dokumencie dodatkowych zagadnień związanych z problematyką przekazywania danych osobowych do państw trzecich (w rozumieniu art. 7 pkt 7 ustawy o ochronie danych osobowych). Chodzi mianowicie o taką nowelizację art. 48 ustawy o ochronie danych osobowych, by umożliwiał on administratorom danych (po spełnieniu przez nich określonych warunków) przekazywanie danych osobowych do państw trzecich bez konieczności każdorazowego uzyskiwania indywidualnej zgody Generalnego Inspektora Ochrony Danych Osobowych.

Istotne zastrzeżenia Generalnego Inspektora pod kątem zgodności z przepisami o ochronie danych osobowych wzbudził również dokument *„Projekt założeń projektu ustawy o szczególnej odpowiedzialności za niektóre naruszenia przepisów ruchu drogowego oraz o zmianie niektórych ustaw”*<sup>138</sup>. Generalny Inspektor wskazał przede wszystkim, że propozycja, by wyjaśnienie właściciela pojazdu wskazujące sprawcę naruszenia przepisów ruchu drogowego, obligatoryjnie zawierało

---

<sup>138</sup> DOLiS-033-583/12

oświadczenie sprawcy o dopuszczeniu się tego naruszenia, pozostaje w oczywistej sprzeczności z wiążącymi Rzeczpospolitą Polską normami prawa międzynarodowego z zakresu problematyki ochrony praw człowieka. Skoro bowiem – jak wskazuje sam projektodawca – z chwilą ustalenia sprawcy naruszenia przepisów ruchu drogowego zastosowane zostanie wobec niego prawo wykroczeń, czyli regulacje z zakresu szeroko rozumianego prawa karnego, to osoba taka podlega ochronie w zakresie przewidzianym zarówno w prawie międzynarodowym, jak i w polskich przepisach prawa. Nie może zaś umknąć uwadze, iż jedną z podstawowych gwarancji przysługujących osobie oskarżonej o popełnienie czynu zabronionego pod groźbą kary jest jej prawo do nieprzymuszania do zeznawania przeciwko sobie lub do przyznania się do winy – art. 14 ust. 3 lit. g Międzynarodowego Paktu Praw Obywatelskich i Politycznych, otwartego do podpisu w Nowym Jorku w dniu 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167 – załącznik). Tymczasem kwestionowane przez organ do spraw ochrony danych osobowych rozwiązanie stanowi w istocie prawny nakaz samooskarżenia się, co jest niezgodne nie tylko z powołanym wyżej aktem prawa międzynarodowego, lecz również z dyspozycją art. 74 § 1 ustawy z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.) w zw. z art. 20 § 3 ustawy z dnia 24 sierpnia 2001 roku – Kodeks postępowania w sprawach o wykroczenia (t. j. Dz. U. z 2008 r. Nr 133, poz. 848 z późn. zm.).

Ponadto Generalny Inspektor podniósł, że w świetle unormowań Konstytucji Rzeczypospolitej Polskiej (w szczególności art. 31 ust. 3 i art. 51 ust. 2) wątpliwości wywołuje także propozycja zmiany art. 78 ustawy z dnia 20 czerwca 1997 roku – Prawo o ruchu drogowym (t. j. Dz. U. z 2012 r. poz. 1137) polegającej na nałożeniu na wszystkich posiadaczy pojazdów obowiązku prowadzenia ewidencji komu i w jakim okresie powierzyli pojazd. Przypomnieć w tym miejscu wypada, że wprowadzenie jakichkolwiek unormowań wkraczających sferę praw i wolności obywatelskich, w tym w gwarantowane konstytucyjnie w art. 47 Konstytucji Rzeczypospolitej Polskiej prawo do prywatności, powinno być poprzedzone przeprowadzeniem testu zgodności tych unormowań z regulacjami konstytucyjnymi. Dopiero pozytywny wynik takiego testu, zgodnie z którym wkroczenie w sferę praw i wolności obywatelskich (np. prawo do prywatności) było niezbędne i adekwatne dla osiągnięcia społecznie oczekiwanego celu, uzasadnia interwencję legislacyjną. W ocenie Generalnego Inspektora Ochrony Danych Osobowych w niniejszej sprawie test taki nie został w ogóle przeprowadzony. Proponowana zmiana art. 78 ustawy – Prawo o ruchu drogowym, nakłada bowiem na kilkanaście milionów obywateli uciążliwy i kosztowny obowiązek bez jakiegokolwiek uzasadnienia. Projektodawca nie wskazał bowiem, która z wymienionych enumeratywnie w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej wartości przemawia za istotnym wkroczeniem w sferę życia prywatnego i rodzinnego kilkunastu milionów obywateli, jakim jest zobligowanie ich do ewidencjonowania dla organów państwa faktów z ich życia osobistego.

Generalny Inspektor zwrócił również uwagę na to, że wspomniana w projekcie założeń zmiana art. 78 ustawy – Prawo o ruchu drogowym, uczyni z owych kilkunastu milionów osób administratorów danych w rozumieniu art. 7 pkt 4 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, którzy będą zobligowani do spełnienia obowiązków przewidzianych w tej ustawie (np. obowiązku stosownego zabezpieczenia przetwarzanych danych, obowiązku rejestracji zbioru danych). Na prawdziwość powyższej tezy wskazuje okoliczność, że w załączonym do projektu założeń teście regulacyjnym na str. 2 pominięto istnienie jakichkolwiek kosztów po stronie obywateli wynikających z wejścia w życie projektowanej ustawy. Jeśli dodać do powyższego, że w projektowanej zmianie art. 78 ustawy – Prawo o ruchu drogowym, nie wskazano również zakresu danych, jakie zawierać ma prowadzona przez każdego posiadacza ewidencja komu i w jakim okresie powierzyli pojazd, to zasadnicza wadliwość rozwiązania zaproponowanego na str. 7 projektu założeń wydawała się bezsporna.

Według stanu na dzień sporządzania niniejszego *Sprawozdania*, ostatnim stanowiskiem wyrażonym w sprawie niniejszego projektu była opinia Rady Legislacyjnej z dnia 22 lutego 2013 r. (znak: RL-0303-1/13), o której wydanie zwróciło się Rządowe Centrum Legislacji pismem z dnia 12 grudnia 2012 r. (znak: RCL.DPŚiL.58-71/12). Rada Legislacyjna w przedmiotowej opinii wyraziła szereg zastrzeżeń i wątpliwości do przedłożonego jej projektu, w szczególności w zakresie celowości wprowadzania proponowanych rozwiązań w odrębnej ustawie, zamiast w drodze nowelizacji ustawy – Prawo o ruchu drogowym.

W przedmiotowym *Sprawozdaniu* należy wspomnieć o opinii Generalnego Inspektora Ochrony Danych Osobowych wyrażonej na temat **projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych**<sup>139</sup>. Nie wchodząc w ocenę zasadności – zaprezentowanego w projekcie ustawy nowelizującej – mechanizmu potwierdzania prawa świadczeniobiorców do uzyskiwania świadczeń opieki zdrowotnej finansowanych ze środków publicznych, Generalny Inspektor stwierdził, że przedstawiona w art. 1 pkt 3 projektu ustawy nowelizującej propozycja brzmienia art. 50 ust. 2 i n. ustawy z dnia 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t. j. Dz. U. z 2008 r. Nr 164, poz. 1027 z późn. zm.), powoływanej dalej z zastosowaniem skrótu „ustawa o świadczeniach”, jest niewystarczająca. O ile bowiem projektowany przepis ustawy o świadczeniach w sposób prawidłowy i wyczerpujący reguluje kształt – wytwarzanej przez Narodowy Fundusz Zdrowia – informacji zwrotnej dotyczącej prawa konkretnego świadczeniobiorcy do świadczeń opieki zdrowotnej finansowanych ze środków publicznych, to nie zawiera jednak niezbędnych unormowań w kwestii zapytania kierowanego przez świadczeniodawcę (osobę uprawnioną w rozumieniu art. 2 pkt 14 ustawy

---

<sup>139</sup> DOLiS-033-71/12/14006

z dnia 12 maja 2011 roku o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych – Dz. U. Nr 122, poz. 696 z późn. zm. niebędącą świadczeniodawcą) do Narodowego Funduszu Zdrowia. Jak zauważył Generalny Inspektor, w szczególności brak jest wskazania, jakie dane świadczeniobiorcy ubiegającego się o świadczenie opieki zdrowotnej ma zawierać takie zapytanie oraz – co wydaje się zdecydowanie istotniejsze z punktu widzenia prawa świadczeniobiorców do ochrony dotyczących ich danych osobowych – w jaki sposób zapewnione ma być, że skierowane do NFZ zapytanie pochodzi od podmiotu uprawnionego (świadczeniodawcy lub osoby uprawnionej w rozumieniu ww. art. 2 pkt 14, niebędącej świadczeniodawcą), nie zaś od innego podmiotu chcącego pozyskać – wskazane w art. 50 ust. 4 ustawy o świadczeniach, w brzmieniu nadanym przez art. 1 pkt 3 projektu ustawy nowelizującej – dane osobowe świadczeniobiorców dla swoich celów. Generalny Inspektor stwierdził, że choć art. 50 ust. 3 ustawy o świadczeniach, w brzmieniu nadanym przez art. 1 pkt 3 projektu ustawy nowelizującej zawiera deklarację, iż wymiana informacji między Narodowym Funduszem Zdrowia a świadczeniodawcami (osobami uprawnionymi w rozumieniu art. 2 pkt 14 ww. ustawy, niebędącymi świadczeniodawcami) ma się odbywać z: „...uwierzytelnieniem stron uprawnionych do przetwarzania tych danych.”, to nie reguluje już kwestii, jak uwierzytelnienie to ma się odbywać, ani nie odsyła w tej kwestii do aktu wykonawczego. Nie negując zasadności rozwiązania zaproponowanego w art. 192 ustawy o świadczeniach, w brzmieniu nadanym przez art. 1 pkt 17 projektu ustawy nowelizującej, to jest przyznania ubezpieczonym prawa do sprawdzenia w Narodowym Funduszu Zdrowia statusu ich prawa do świadczeń opieki zdrowotnej finansowanych ze środków publicznych, Generalny Inspektor zwrócił uwagę, że nie zostało ono dopracowane. W projekcie ustawy nowelizującej nie znalazły się bowiem żadne przepisy regulujące sposób, w jaki ubezpieczony może skorzystać z tego nowego uprawnienia (dotyczące np. formy wniosku, sposobu jego składania, terminu w jakim NFZ winien się do niego ustosunkować, itp.). Podczas kolejnych etapów procesowania ww. aktu prawnego, w nawiązaniu do dyskusji przeprowadzonej na konferencji uzgodnieniowej, która odbyła się w dniu 29 marca 2012 roku, Generalny Inspektor podtrzymał przedstawione uwagi. W kolejnym piśmie zawierającym uwagi odnośnie ww. projektu zaznaczył, iż – zaprezentowane w dokumencie „Uwagi do ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych uzgodnienia międzyresortowe” – nowe brzmienie art. 50 ust. 3 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.) nie rozstrzyga wszystkich wątpliwości podniesionych we wcześniejszej korespondencji z Ministerstwem Administracji i Cyfryzacji. Generalny Inspektor podniósł, że o ile przyjmie – zaproponowane w projektowanym przepisie – rozwiązanie, zgodnie z którym świadczeniodawca lub niebędąca świadczeniodawcą osoba uprawniona w rozumieniu art. 2 pkt 14 ustawy z dnia 12 maja 2011 roku o refundacji leków, środków spożywczych specjalnego przeznaczenia

żywnościowego oraz wyrobów medycznych, występujący do Narodowego Funduszu Zdrowia z zapytaniem, czy osoba ubiegająca się o świadczenie zdrowotne jest objęta ubezpieczeniem zdrowotnym, będą posługiwać się w tym zapytaniu numerem PESEL osoby ubiegającej się o świadczenie zdrowotne, to w dalszym ciągu aktualny pozostaje problem zapewnienia, by zapytanie takie pochodziło od podmiotu uprawnionego (to jest świadczeniodawcy lub niebędącej świadczeniodawcą osoby uprawnionej w rozumieniu art. 2 pkt 14 ww. ustawy o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych). Generalny Inspektor uznał, że ze względu na stosunkowo dużą łatwość pozyskiwania numerów PESEL zarysowany wyżej problem nabiera szczególnego znaczenia. Dlatego Generalny Inspektor podtrzymał stanowisko, co do potrzeby uzupełnienia projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych o regulacje odnoszące się do zasad uwierzytelniania się podmiotów uprawnionych i gwarantujące integralność oraz poufność przetwarzanych danych. Jako przykład takich regulacji wskazał unormowania zawarte w rozdziale 4 i 5 ustawy z dnia 15 kwietnia 2011 roku o systemie informacji oświatowej (Dz. U. Nr 139, poz. 814 z późn. zm.). Generalny Inspektor wspominał również, że w wypadku, gdyby projektodawca podtrzymywał przedstawiony na konferencji uzgodnieniowej pogląd, w myśl którego nowe ujęcie dyspozycji art. 50 ust. 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych stanowi wystarczającą gwarancję niemożliwości skutecznego kierowania przez podmioty nieuprawnione zapytań do NFZ o objęciu (nieobjęciu) konkretnej osoby ubezpieczeniem zdrowotnym, to przypomnieć należy, że zgodnie z art. 97 ust. 3 pkt 8 i ust. 4 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, NFZ jest administratorem danych zgromadzonych w Centralnym Wykazie Ubezpieczonych i ponosi pełną odpowiedzialność za ochronę przetwarzanych danych. Podkreślił również, że nie można przy tym wykluczyć, że następstwem takiego działania NFZ może być wydanie przez Generalnego Inspektora Ochrony Danych Osobowych – w oparciu o art. 18 ust. 1 ustawy o ochronie danych osobowych – decyzji administracyjnej zakazującej przekazywania z Centralnego Wykazu Ubezpieczonych informacji o objęciu (nieobjęciu) konkretnej osoby ubezpieczeniem zdrowotnym. Aktualne więc pozostaje – zaprezentowane w piśmie z dnia 8 marca 2012 roku - stanowisko odnośnie potrzeby określenia zasad dokonywania zapytań i uwierzytelniania się świadczeniobiorców w systemie informatycznym NFZ celem pozyskania informacji o posiadanym prawie do świadczeń opieki zdrowotnej. W opinii GODO względ na potrzebę zabezpieczenia danych osobowych wielu milionów świadczeniobiorców jednoznacznie przemawia za wprowadzeniem do ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, unormowań gwarantujących bezpieczeństwo systemu informatycznego NFZ, uniemożliwiających dostęp do tego systemu osobom nieuprawnionym.

W tym miejscu podkreślenia wymaga, że także na etapie prac sejmowych Generalny Inspektor nadal przedstawiał swoje uwagi do omawianego projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (druk sejmowy nr 489)<sup>140</sup>. Odwołując się do wcześniejszego etapu prac legislacyjnych wskazał, że w następstwie konsultacji przyjęto – postulowane przez Generalnego Inspektora Ochrony Danych Osobowych – rozwiązanie, zgodnie z którym warunki, jakie musi spełniać świadczeniodawca lub niebędąca świadczeniodawcą osoba uprawniona w rozumieniu art. 2 pkt 14 ustawy z dnia 12 maja 2011 roku o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych występująca do Narodowego Funduszu Zdrowia o dokument elektroniczny potwierdzający prawo świadczeniobiorcy do świadczeń opieki zdrowotnej, będą określone przez ministra właściwego do spraw zdrowia w drodze rozporządzenia, w brzmieniu nadanym przez art. 1 pkt 3 projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Przedmiotem wątpliwości Generalnego Inspektora pozostał art. 192 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w brzmieniu nadanym przez art. 1 pkt 20 analizowanego projektu ustawy. Generalny Inspektor nie negował zasadności i celowości rozwiązania zaproponowanego w tym przepisie, a mianowicie przyznania każdemu świadczeniobiorcy prawa do sprawdzenia w NFZ, na podstawie informacji przetwarzanych w Centralnym Wykazie Ubezpieczonych, czy przysługuje mu prawo do świadczeń opieki zdrowotnej. Zauważył jednak, iż projektowana regulacja jest niepełna. W kwestionowanym unormowaniu nadal brak było wskazania, w jaki sposób świadczeniobiorca może skorzystać z tego uprawnienia, jak również przepisów gwarantujących bezpieczeństwo systemu informatycznego NFZ i uniemożliwiających pozyskanie z tego systemu informacji przez osoby nieuprawnione (np. regulujących sposób potwierdzania przez NFZ, że żądanie informacji o prawie do świadczeń opieki zdrowotnej konkretnego świadczeniobiorcy pochodzi rzeczywiście od tego świadczeniobiorcy).

W kolejnej opinii do projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Generalny Inspektor poinformował, że spośród nadesłanych wersji brzmienia tego przepisu, możliwa do akceptowania była wersja wcześniejsza (z dnia 17 lipca 2012 roku) w brzmieniu: „2. *Minister właściwy do spraw zdrowia, po zasięgnięciu opinii Prezesa Funduszu, określi, w drodze rozporządzenia sposób identyfikacji świadczeniobiorców występujących o informacje, o których mowa w ust. 1 oraz sposób, tryb i terminy udostępniania świadczeniobiorcom przez Fundusz tych informacji, mając na uwadze zakres informacji o jaką występuje świadczeniobiorca oraz konieczność zapewnienia ochrony danych osobowych świadczeniobiorców przed nieuprawnionym dostępem lub ujawnieniem*”.

---

<sup>140</sup> DOLiS-033-330/12/ 41200

Wersja późniejsza (z 18 i 19 lipca 2012 roku) nie zawierała jednego z elementów, którego potrzebę unormowania Generalny Inspektor wskazywał w piśmie z dnia 4 lipca 2012 roku. Mianowicie brakowało w niej określenia sposobu „(...) *potwierdzania przez NFZ, że żądanie informacji o prawie do świadczeń opieki zdrowotnej konkretnego świadczeniobiorcy pochodzi rzeczywiście od tego świadczeniobiorcy...*”. Wersja ta nie nakładała na ministra właściwego do spraw zdrowia obowiązku uregulowania w rozporządzeniu sposobu identyfikacji przez Narodowy Fundusz Zdrowia świadczeniobiorców występujących o informacje, o których mowa w ust. 1 art. 192 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

Ostatecznie Generalny Inspektor wskazał, że wersja zawierająca roboczą propozycję brzmienia art. 192 ust. 2 ustawy o świadczeniach, w brzmieniu: „2. *Minister właściwy do spraw zdrowia, po zasięgnięciu opinii Prezesa Funduszu, określi, w drodze rozporządzenia sposób, tryb i terminy występowania do Funduszu oraz udostępniania przez Fundusz informacji, o których mowa w ust. 1, mając na uwadze zakres informacji, o jaką występuje świadczeniobiorca, konieczność zapewnienia właściwej identyfikacji i uwierzytelniania świadczeniobiorcy oraz ochrony danych osobowych przed nieuprawnionym dostępem lub ujawnieniem.*” zasługuje na akceptację Generalnego Inspektora Ochrony Danych Osobowych<sup>141</sup>.

Odnosząc się natomiast do **projektu ustawy o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw**<sup>142</sup> Generalny Inspektor uznał za istotne trzy kwestie: zasada obowiązkowej retencji danych telekomunikacyjnych, obowiązek powiadamiania właściwego organu krajowego odpowiedzialnego za ochronę danych osobowych oraz abonentów lub użytkowników końcowych będących osobami fizycznymi o naruszeniu ich danych osobowych, a także przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego (tzw. „cookies”).

Odnosząc się do nowelizacji przepisów o obowiązkowej retencji danych telekomunikacyjnych, Generalny Inspektor stwierdził, że choć uznać należy za krok w dobrym kierunku propozycję skrócenia do 12 miesięcy<sup>143</sup> okresu przechowywania przez operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych danych, o których mowa w art. 180 c ustawy – Prawo telekomunikacyjne, to zakres przedłożonej nowelizacji przepisów regulujących tzw. „retencję danych” jest zbyt wąski. W opinii Generalnego Inspektora samo skrócenie okresu przechowywania tzw. „danych retencyjnych” (z 24 do 12 miesięcy) nie było rozwiązaniem

---

<sup>141</sup> Ustawę o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych uchwalono w dniu 27 lipca 2012 r. (Dz. U. z 2012 r. poz. 1016).

<sup>142</sup> DOLiS-033-378/12

<sup>143</sup> art. 180 a ust. 1 pkt 1 ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.), w brzmieniu nadanym przez art. 1 pkt 118 projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (druk sejmowy nr 627).

wystarczającym, gdyż w dalszym ciągu brak było w opisywanym projekcie unormowań zmierzających do zapewnienia racjonalnego wykorzystywania tych danych. W szczególności nie znalazła odzwierciedlenia wytyczna zamieszczona w dyrektywie 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 roku w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE (Dz. Urz. UE L 105 z 13.04.2006, str. 54), zgodnie z którą zatrzymywanie danych retencyjnych powinno być dokonywane w celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego. Generalny Inspektor przypomniiał, że wobec niewprowadzenia do polskiego ustawodawstwa takiego ograniczenia dopuszczalności wykorzystywania danych retencyjnych, zdarzają się sytuacje występowania o takie dane na potrzeby postępowań cywilnych (np. w sprawach o rozwód). W ocenie Generalnego Inspektora nieprzyjęcie koncepcji, zgodnie z którą dane retencyjne powinny być wykorzystywane jedynie dla celów wykrywania i ścigania sprawców poważnych przestępstw, było jedną z przyczyn tak wielkiej liczby wniosków o udostępnienie danych retencyjnych kierowanych w każdym roku przez uprawnione podmioty do operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych.

Generalny Inspektor pozytywnie ocenił zaproponowany przez projektodawcę w art. 174 a – art. 174 d ustawy – Prawo telekomunikacyjne (dodany przez art. 1 pkt 113 projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw), sposób implementacji postanowień dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 roku dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. UE L 201 z 31.07.2002, str. 37 z późn. zm.) zwanej dyrektywą o prywatności i łączności elektronicznej, w zakresie obowiązku powiadamiania właściwego organu krajowego odpowiedzialnego za ochronę danych osobowych (w Rzeczypospolitej Polskiej – Generalnego Inspektora Ochrony Danych Osobowych) oraz abonentów lub użytkowników końcowych będących osobami fizycznymi, o naruszeniu danych osobowych tych abonentów (użytkowników końcowych). Generalny Inspektor zaznaczył, że przedłożone do zaopiniowania regulacje odnoszące się do procedury notyfikacji naruszeń stanowią wynik długotrwałych uzgodnień z organem do spraw ochrony danych osobowych i uwzględniają sugestie Generalnego Inspektora zgłaszane w trakcie tych konsultacji.

Oprócz tego Generalny Inspektor poinformował, iż w art. 174 a ust. 8 *in principio* ustawy – Prawo telekomunikacyjne (dodanym przez art. 1 pkt 113 projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw) znalazło się nieprawidłowe odesłanie do ust. 2 art. 174 a ustawy – Prawo telekomunikacyjne zamiast do ust. 3 tego przepisu. Jeśli zaś chodzi o przedstawioną propozycję (art. 173 ustawy – Prawo telekomunikacyjne, w brzmieniu nadanym przez art. 1 pkt 112 projektu ustawy o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych



ustaw) zmiany unormowań dotyczących przechowywania informacji lub uzyskiwania dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego (tzw. „cookies”), to – jak wskazał Generalny Inspektor – stanowi ona kompromis pomiędzy wyrażanymi w doktrynie poglądami skrajnymi, zgodnie z którymi „cookies” wymagają wyrażonej zgody abonenta (użytkownika końcowego), a poglądami bardziej liberalnymi, uwzględniającymi interesy dostawców usług. Podkreślić należy, iż stanowisko Komisji Europejskiej co do sposobu interpretacji postanowień art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej również ewaluowało (od wymagania posiadania wyrażonej zgody abonenta w kierunku pewnej liberalizacji tego wymogu), zaś kwestia zgody w odniesieniu do „cookies” w dalszym ciągu pozostaje przedmiotem ożywionych dyskusji. W tej kwestii wypada choćby wspomnieć Opinię Nr 4/2012 Grupy Roboczej Art. 29 z dnia 7 czerwca 2012 r. w sprawie wyjątków w zakresie pozyskiwania zgody na zapisywanie plików cookie. W tym stanie rzeczy przedłożona propozycja brzmienia art. 173 ustawy – Prawo telekomunikacyjne uznana została przez GODO przy założeniu, że projektowany art. 173 ust. 2 ustawy – Prawo telekomunikacyjne będzie interpretowany w ten sposób, że dla przyjęcia istnienia zgody abonenta (użytkownika końcowego) niezbędne będzie dokonanie przez niego stosownych ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub dokonanie przez niego konfiguracji usługi<sup>144</sup>.

Formułując swoje uwagi do *projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw* Generalny Inspektor wskazał, że użycie w projektowanym (art. 2 pkt 2 projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw) art. 20 a ust. 1 pkt 2, ust. 3 pkt 2 oraz ust. 4 ustawy z dnia 24 maja 2000 roku o Krajowym Rejestrze Karnym (t. j. Dz. U. z 2012 r. poz. 654) nowego, niezdefiniowanego pojęcia „dane (danych) o orzeczeniu”, może budzić uzasadnione wątpliwości. Dotychczas obowiązująca ustawa o Krajowym Rejestrze Karnym nie posługiwała się takim terminem, a we wszystkich przypadkach, gdy przewidywała przetwarzanie danych o zapadłym orzeczeniu, szczegółowo normowała katalog podlegających przetwarzaniu informacji o tym orzeczeniu (np. art. 12 ust. 1 pkt 2 – 6, art. 12 ust. 1 pkt 6 c, art. 12 ust. 1 a pkt 2 – 5 ustawy o Krajowym Rejestrze Karnym). Tymczasem – z przyczyn nieznanych organowi do spraw ochrony danych osobowych – w proponowanym w art. 2 pkt 2 omawianego projektu, brzmieniu art. 20 a ust. 1 pkt 2, ust. 3 pkt 2 oraz ust. 4 ustawy o Krajowym Rejestrze Karnym, projektodawca odstąpił od tego prawidłowego, w opinii GODO, rozwiązania i posłużył się kategorią zbiorczą – „dane o orzeczeniu”. Zdaniem Generalnego Inspektora w oparciu o analizę tak skonstruowanego przepisu ustawy o Krajowym Rejestrze Karnym, nie można w istocie

---

<sup>144</sup> Zmiana przepisów Prawa telekomunikacyjnego nastąpiła wraz z ogłoszeniem w Dzienniku Ustaw z dnia 21 grudnia 2012 r. ustawy z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. z 2012 r. poz. 1445).

stwierdzić, o jakie informacje o orzeczeniu chodzi. Takie ujęcie dyspozycji przepisu regulującego przetwarzanie danych szczególnie chronionych (w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych) nie było w ocenie organu do spraw ochrony danych osobowych prawidłowe i winno być zmienione, choćby poprzez zastosowanie odpowiednich odesłań jak przykładowo przewidziano to w art. 12 ust. 2 b i ust. 2 c ustawy o Krajowym Rejestrze Karnym. Niezależnie od powyższego Generalny Inspektor poinformował, że projektowany (art. 1 pkt 1 projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw) art. 21 ust. 3 pkt 1 ustawy z dnia 20 sierpnia 1997 roku o Krajowym Rejestrze Sądowym (t. j. Dz. U. z 2007 r. Nr 168, poz. 1186 z późn. zm.) zawiera w swojej treści odesłanie do art. 585 ustawy z dnia 15 września 2000 roku – Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037 z późn. zm.), który to przepis został uchylony w 2011 roku przez art. 3 ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 133, poz. 767).

W kolejnej korespondencji<sup>145</sup> Generalny Inspektor wskazał, że w odpowiedzi na pismo z dnia 27 września 2012 roku<sup>146</sup> dotyczące nowej wersji z dnia 27.09.2012 r. projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw, organ do spraw ochrony danych osobowych akceptuje sposób uwzględnienia przez projektodawcę zasadniczej uwagi (do art. 20 a ust. 1 pkt 2, ust. 3 pkt 2 oraz ust. 4 ustawy z dnia 24 maja 2000 roku o Krajowym Rejestrze Karnym – t. j. Dz. U. z 2012 r. poz. 654, dodanych przez art. 2 pkt 2 projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw) zawartej w jego piśmie z dnia 18 września 2012 roku<sup>147</sup>. Jeśli zaś chodzi o zgłoszone zastrzeżenie wobec brzmienia art. 21 ust. 3 pkt 1 ustawy z dnia 20 sierpnia 1997 roku o Krajowym Rejestrze Sądowym (t. j. Dz. U. z 2007 r. Nr 168, poz. 1186 z późn. zm.) dodawanego przez art. 1 pkt 1 projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw, to uwaga Generalnego Inspektora Ochrony Danych Osobowych miała charakter jedynie techniczno-legislacyjny i dotyczyła zamieszczenia w projektowanym przepisie odesłania do nieobowiązującego unormowania z art. 585 ustawy z dnia 15 września 2000 roku – Kodeks spółek handlowych (Dz. U. Nr 94, poz. 1037 z późn. zm.). Skoro z przyczyn merytorycznych odesłanie takie było – w opinii projektodawcy – zasadne, organ do spraw ochrony danych osobowych nie zgłosił wątpliwości wobec sposobu ujęcia dyspozycji art. 21 ust. 3 pkt 1 ustawy o Krajowym Rejestrze Sądowym. Wobec wyczerpującego ustosunkowania się przez projektodawcę do wszystkich zastrzeżeń zawartych w piśmie Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 września 2012 roku, organ do spraw ochrony danych osobowych uznał projekt ustawy o zmianie

---

<sup>145</sup> DOLiS-033-428/12/59389

<sup>146</sup> znak: DPrC - III - 4392-15/12

<sup>147</sup> DOLiS-033-428/12/TG/56661

ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw (w wersji z dnia 27.09.2012 r.) za uzgodniony.

W swoim kolejnym piśmie dotyczącym tego projektu, Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę na ograniczony zakres konsultacji projektu z organem do spraw ochrony danych osobowych. Przedmiotowy projekt powstał bowiem z połączenia procedowanych oddzielnie, projektów *ustawy o zmianie ustawy o Krajowym Rejestrze Karnym i ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw*. Zauważyć zaś należy, że – wbrew dyspozycji art. 12 pkt 5 ustawy o ochronie danych osobowych w zw. z § 12 ust. 4 uchwały Nr 49 Rady Ministrów z dnia 19 marca 2002 roku – Regulamin pracy Rady Ministrów (M. P. Nr 13, poz. 221 z późn. zm.), żaden z tych projektów nie został przedstawiony do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych. W przypadku *projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw*, organ do spraw ochrony danych osobowych informację o nim pozyskał z własnej inicjatywy (z Biuletynu Informacji Publicznej Rządowego Centrum Legislacji) i pismem z dnia 18 września 2012 r. zdecydował się wnieść do niego uwagi<sup>148</sup>. Pismo to zainicjowało wymianę korespondencji, w następstwie której uwagi organu do spraw ochrony danych osobowych zostały zasadniczo uwzględnione - nowe brzmienie art. 20 a z dnia 24 maja 2000 roku o Krajowym Rejestrze Karnym (t. j. Dz. U. z 2012 r. poz. 654). Natomiast jeśli chodzi o projekt *ustawy o zmianie ustawy o Krajowym Rejestrze Karnym*, to do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął jedynie dokument „Założenia do projektu ustawy o zmianie ustawy o Krajowym Rejestrze Karnym” do którego to dokumentu organ do spraw ochrony danych osobowych zgłosił uwagi, jak również zwrócił się do Ministerstwa Sprawiedliwości pismem z dnia 11 maja 2012 r. o wskazanie podstawy prawnej dla tworzenia – sygnalizowanego w tym dokumencie – „projektowanego systemu zarządzania tożsamością w sądach powszechnych”<sup>149</sup>. Do powyższego pisma organu do spraw ochrony danych osobowych Ministerstwo Sprawiedliwości nie ustosunkowało się, choć treść jego była mu znana, na co wskazuje dyspozycja dodawanego art. 6 ust. 1 pkt 10 a ustawy o Krajowym Rejestrze Karnym. Co więcej, powstały w oparciu o te założenia projekt *ustawy o zmianie ustawy o Krajowym Rejestrze Karnym* nie został przesłany do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych. Jeśli dodać do powyższego, że również będący przedmiotem niniejszej opinii projekt nie wpłynął do Biura GODO, pomimo iż reguluje bezpośrednio kwestię przetwarzania danych dotyczących skazań, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym, czyli danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, to uzasadnione wydaje się stwierdzenie, iż dotychczasowa współpraca między Ministerstwem Sprawiedliwości a organem do spraw ochrony danych osobowych

---

<sup>148</sup> DOLiS-033-428/12/TG/56661

<sup>149</sup> DOLiS-033-227/12/TG/29328

w odniesieniu do, proponowanych przez to Ministerstwo w projekcie (i poprzedzającym go projekcie *ustawy o zmianie ustawy o Krajowym Rejestrze Karnym*), zmian ustawy o Krajowym Rejestrze Karnym, nie była wystarczająca. W tym stanie rzeczy, wobec przewidzianego w projekcie (art. 1 pkt 5 lit. a) brzmienia (dodawanego) art. 12 ust. 1 b ustawy o Krajowym Rejestrze Karnym, który to przepis statuuje stosowanie przy przetwarzaniu danych w Krajowym Rejestrze Karnym tzw. „sądowego podpisu elektronicznego”, Generalny Inspektor Ochrony Danych Osobowych ponowił (zamieszczone już w piśmie z dnia 11 maja 2012 roku<sup>150</sup>) pytanie o podstawę prawną dla wprowadzenia takiego rozwiązania. Z załączonego do projektu, lakonicznego w tej części, uzasadnienia wynikało bowiem jedynie, że przedmiotowy „sądowy podpis elektroniczny” stanowi „projektowany system zarządzania tożsamością w sądach powszechnych”. Tymczasem organowi do spraw ochrony danych osobowych nie jest znany jakikolwiek akt prawny, który regulowałby zasady wprowadzenia w sądach powszechnych takiego „systemu zarządzania tożsamością”, który to system, w zamierzeniach Ministerstwa Sprawiedliwości, miałby stanowić alternatywę wobec rozwiązań przyjętych w ustawie z dnia 18 września 2001 roku o podpisie elektronicznym (Dz. U. Nr 130, poz. 450, z późn. zm.). Z powyższych względów Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Sprawiedliwości o wskazanie stosownych unormowań regulujących zasady nadawania i stosowania „sądowego podpisu elektronicznego”, jak również o wyjaśnienie stosunku tych unormowań do przepisów ustawy o podpisie elektronicznym.

W kolejnej korespondencji dotyczącej tego projektu Generalny Inspektor poinformował, że akceptuje brzmienie przedmiotowej ustawy zamieszczone w druku senackim nr 262, a w szczególności nową dyspozycję art. 12 ust. 1 b ustawy z dnia 24 maja 2000 roku o Krajowym Rejestrze Karnym (t. j. Dz. U. z 2012 r. poz. 654), dodawanego przez art. 1 pkt 5 lit. a ustawy z dnia 7 grudnia 2012 roku o zmianie ustawy o Krajowym Rejestrze Karnym oraz niektórych innych ustaw. Tym samym wyżej wskazaną wersję projektu ustawy uznał za uzgodnioną z organem do spraw ochrony danych osobowych<sup>151</sup>.

Kolejna istotna opinia Generalnego Inspektora Ochrony Danych Osobowych dotyczyła ***projektu ustawy o zmianie ustawy o opiece nad dziećmi w wieku do lat 3 oraz niektórych innych ustaw***<sup>152</sup>. Poważne wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budziła przede wszystkim dyspozycja nowego art. 6 a ustawy o opiece nad dziećmi w wieku do lat 3. W ocenie organu do spraw ochrony danych osobowych sformułowanie tego przepisu nie tylko bowiem narusza, wprowadzoną 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, lecz również może powodować istotne

---

<sup>150</sup> Ibidem

<sup>151</sup> Projekt ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw został uchwalony w dniu 7 grudnia 2012 r. i został ogłoszony w Dz. U. z dnia 29 grudnia 2012 r. (Dz. U. z 2012 r. poz. 1514).

<sup>152</sup> DOLiS-033-445/12

trudności praktyczne. Projektowany przepis wprowadzał nieznanym innym ustawom, obowiązek posiadania adresu poczty elektronicznej oraz numeru telefonu przez rodzica ubiegającego się o objęcie jego dziecka (dzieci) opieką w żłobku lub klubie dziecięcym albo przez dziennego opiekuna. Taki sposób rozumienia przedmiotowego przepisu wynika wprost z użytego w nim sformułowania: „jest zobowiązany do przedstawienia następujących danych [...] 4) adres poczty elektronicznej i numer telefonu rodziców”. Nie negując prawa projektodawcy do nakładania na obywateli obowiązków w przepisach rangi ustawowej (przy spełnieniu wymagań z art. 36 ust. 3 Konstytucji Rzeczypospolitej Polskiej) Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, że projektowany przepis może mieć potencjalnie charakter dyskryminujący (zwłaszcza wobec osób objętych tzw. „wykluczeniem cyfrowym”). Jeszcze większe zastrzeżenia budził projektowany art. 6 a ust. 1 pkt 5 ustawy o opiece nad dziećmi w wieku do lat 3 odczytywany w powiązaniu z – komentowanym już – art. 6 a ust. 1 zdanie wstępne tejże ustawy. Analiza literalnego brzmienia tego przepisu prowadziła bowiem do wniosku, iż warunkiem *sine qua non* ubiegania się o objęcie dziecka opieką w żłobku lub klubie dziecięcym albo przez dziennego opiekuna jest pozostawanie w stosunku zatrudnienia przez obydwoje jego rodziców („jest zobowiązany do przedstawienia następujących danych [...] 5) miejsce pracy rodziców”). Organowi do spraw ochrony danych osobowych trudno było przyjąć, że taki był rzeczywisty zamiar projektodawcy, jednakże w aktualnym brzmieniu krytykowany przepis nie może być odczytany inaczej, aniżeli w sposób wyżej wskazany.

Powołując się również na zasadę adekwatności przetwarzanych danych w stosunku do celów ich przetwarzania, Generalny Inspektor Ochrony Danych Osobowych zakwestionował również pozyskiwanie danych o tak prywatnym charakterze, jakimi są informacje o wysokości dochodów rodziców dziecka, które ma być objęte opieką w żłobku lub klubie dziecięcym albo przez dziennego opiekuna (art. 6 a ust. 1 pkt 8 ustawy o opiece nad dziećmi w wieku do lat 3). Wskazał, że jeśli zaś chodzi o miejsce opłacania podatku dochodowego od osób fizycznych przez rodziców (art. 6 ust. 1 pkt 7 ustawy o opiece nad dziećmi w wieku do lat 3), to – zgodnie z art. 17 § 1 ustawy z dnia 29 sierpnia 1997 roku – Ordynacja podatkowa (t. j. Dz. U. z 2012 r. poz. 749) i § 4 ust. 2 rozporządzenia Ministra Finansów z dnia 22 sierpnia 2005 roku w sprawie właściwości organów podatkowych (Dz. U. Nr 165, poz. 1371 z późn. zm.) – jest ono uzależnione od miejsca wspólnego zamieszkania rodziców dziecka, zaś w przypadku gdy mają oni różne miejsca zamieszkania, a – na ich wniosek – podlegają łącznemu opodatkowaniu, od miejsca zamieszkania jednego z nich. Informacje zaś odnośnie miejsca zamieszkania rodziców dziecka, które ma być objęte opieką w żłobku lub klubie dziecięcym albo przez dziennego opiekuna mogą być pozyskiwane już na podstawie (niekwestionowanego przez organ do spraw ochrony danych osobowych) art. 6 ust. 1 pkt 3 ustawy o opiece nad dziećmi w wieku do lat 3

(dodawanego przez art. 1 pkt 2 ustawy nowelizującej). W istocie zatem proponowany art. 6 ust. 1 pkt 7 ustawy o opiece nad dziećmi w wieku do lat 3 jawił się jako zbędny<sup>153</sup>.

Nie sposób nie wspomnieć w niniejszym *Sprawozdaniu* o opinii GIODO dotyczącej **projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw**<sup>154</sup>. W odniesieniu do tego projektu GIODO zwrócił uwagę, że budzić musi pewne zdziwienie sytuacja, w której projekt dotyczących bezpośrednio problematyki przetwarzania danych dotyczących skazań, czyli danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, nie został, wbrew jednoznacznej dyspozycji art. 12 pkt 5 ustawy o ochronie danych osobowych, przedłożony do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych. W zakresie merytorycznej oceny rozwiązań zaproponowanych w projekcie, w pierwszej kolejności Generalny Inspektor wyraził zastrzeżenia co do propozycji (art. 1 pkt 1 projektu) wprowadzenia w ustawie z dnia 6 czerwca 1997 roku – Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.) nowego środka zabezpieczającego nazwanego przez projektodawcę „podaniem wyroku do publicznej wiadomości” (dodawany przez art. 1 pkt 1 projektu art. 92 b §1 pkt 1 ustawy – Kodeks karny). Zaproponowana w przedmiotowym przepisie konstrukcja prawna była kontrowersyjna, mogła pozostawać w sprzeczności z zasadami prawa karnego, zaś praktyczne jej zastosowanie wywołać skutki nieprzewidziane przez projektodawcę. Ponadto już wstępna analiza projektowanego art. 92 b § 1 pkt 1 ustawy – Kodeks karny, w powiązaniu z projektowanymi art. 92 c § 1 ustawy – Kodeks karny i art. 98 a ustawy – Kodeks karny, wskazuje jednoznacznie na pewne istotne nieporozumienie. Skoro bowiem – przewidziane w projektowanym art. 92 b § 1 pkt 1 ustawy – Kodeks karny – „podanie wyroku do publicznej wiadomości” ma nastąpić: „bezpośrednio po zakończeniu odbywania przez sprawcę orzeczonej kary pozbawienia wolności lub przy warunkowym odstąpieniu od umieszczenia sprawcy w zakładzie psychiatrycznym lub innym zakładzie zamkniętym” (projektowany art. 98 a § 2 ustawy – Kodeks karny), to w istocie środek ten (w takiej postaci) nie jest podaniem wyroku do publicznej wiadomości, lecz skierowaną do społeczeństwa informacją o zakończeniu odbywania kary (odzyskaniem wolności w inny prawny sposób) przez sprawcę – określonych w projektowanym art. 98 a § 1 ustawy – Kodeks karny – przestępstw. Jeśli zaś, zgodnie z projektowanym art. 92 c § 1 ustawy – Kodeks karny, środek zabezpieczający orzeka sąd w celu zapobieżenia popełnieniu przez sprawcę czynu zabronionego o znacznej społecznej szkodliwości, to rodzi się zasadnicze pytanie, w jaki sposób poinformowanie społeczeństwa o odzyskaniu wolności przez sprawcę określonych przestępstw ma zapobiec popełnieniu przez niego kolejnego czynu zabronionego. Nie jest przecież celem projektodawcy nakłanianie

---

<sup>153</sup> Ustawa o zmianie ustawy o opiece nad dziećmi w wieku do lat 3 oraz niektórych innych ustaw została uchwalona w dniu 10 maja 2013 r., zaś w dniu 13 maja ustawę przekazano Prezydentowi i Marszałkowi Senatu.

<sup>154</sup> DOLiS-033-564/12

społeczeństwa do samodzielnego podejmowania działań wobec sprawców niektórych przestępstw w imię zasady „ochrony społeczeństwa”.

Generalny Inspektor zwrócił uwagę, że projektodawcy umknęło także (na co wskazuje pominięcie w przepisach dotyczących środka zabezpieczającego nazwanego przez projektodawcę „podaniem wyroku do publicznej wiadomości” regulacji zamieszczonej w części końcowej obowiązującego art. 50 ustawy – Kodeks karny), iż w pewnych okolicznościach podanie do wiadomości publicznej informacji o skazaniu za przestępstwo (zwłaszcza z katalogu przestępstw przeciwko wolności seksualnej) skutkować może nienaprawialną szkodą dla osoby pokrzywdzonej tym przestępstwem powodując jej stygmatyzację. Z tych wszystkich przyczyn, w opinii organu do spraw ochrony danych osobowych, zaproponowane rozwiązanie polegające na wprowadzeniu środka zabezpieczającego nazwanego „podaniem wyroku do publicznej wiadomości” budziło wątpliwości z punktu widzenia – przewidzianych w Konstytucji Rzeczypospolitej Polskiej – zasad niezbędności i proporcjonalności. Przypomnieć zaś należy, że wprowadzenie jakichkolwiek unormowań ograniczających sferę praw i wolności obywatelskich powinno być poprzedzone przeprowadzeniem testu zgodności tych unormowań z regulacjami konstytucyjnymi. Dopiero pozytywny wynik takiego testu, zgodnie z którym wkroczenie w sferę praw i wolności obywatelskich (np. prawo do prywatności) jest niezbędne i adekwatne dla osiągnięcia społecznie oczekiwanego celu, uzasadnia interwencję legislacyjną. W ocenie Generalnego Inspektora Ochrony Danych Osobowych w niniejszej sprawie test taki nie został przeprowadzony gruntownie.

Wątpliwości organu do spraw ochrony danych osobowych budziła również dyspozycja art. 17 projektu. Z jednej strony bowiem projektodawca nie wskazał w przedmiotowym przepisie kryteriów, na podstawie których pracodawca winien zwrócić się do Krajowego Rejestru Karnego o informacje o pracowniku zatrudnionym przy pracach związanych ze stałymi i bezpośrednimi kontaktami z małoletnimi. Odczytując literalnie proponowany przepis informacją, która obligowałaby pracodawcę do podjęcia działań (wystąpienia z zapytaniem do Krajowego Rejestru Karnego), mogłaby być bowiem choćby plotka, czy też pomówienie, co nie wydaje się rozwiązaniem racjonalnym. Z drugiej zaś – zaproponowana w art. 17 ust. 2 projektu obligatoryjna sankcja w postaci rozwiązania stosunku pracy bez wypowiedzenia z winy pracownika jawi się jako wątpliwa. Zauważyć bowiem należy, iż dopiero niniejszy projekt ustawy wprowadza w art. 16 wymóg niekaralności za przestępstwa przeciwko wolności seksualnej i obyczajności oraz przestępstwa przeciwko prawidłowemu rozwojowi psychoseksualnemu małoletnich w odniesieniu do osób zatrudnionych przy pracach związanych ze stałymi i bezpośrednimi kontaktami z małoletnimi. Tak więc dopiero od dnia wejścia w życie przedmiotowego projektu jako obowiązującej ustawy, skazanie za przestępstwo przeciwko wolności seksualnej i obyczajności oraz za przestępstwo przeciwko prawidłowemu rozwojowi psychoseksualnemu małoletnich, stanowić będzie dla pracownika zatrudnionego przy pracach

związanych ze stałymi i bezpośrednimi kontaktami z małoletnimi zawinioną utratę uprawnień w rozumieniu art. 52 §1 pkt 3 ustawy z dnia 26 czerwca 1974 roku – Kodeks pracy (t. j. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.).

Prace legislacyjne nad projektem toczyły się również w 2013 r. Do Generalnego Inspektora Ochrony Danych Osobowych w kwietniu 2013 r. trafiła kolejna wersja projektu – zatytułowana **„Projekt ustawy o postępowaniu wobec osób zaburzonych psychicznie stwarzających zagrożenie dla życia, zdrowia lub wolności seksualnej innych osób”** – wobec której GIODI zajął odpowiednie stanowisko<sup>155</sup>.

Interesującą opinię Generalny Inspektor Ochrony Danych Osobowych wydał wobec projektu **rozporządzenia Ministra Sprawiedliwości w sprawie przeprowadzania konkursu na stanowisko asystenta sędziego**<sup>156</sup>. W opinii tej Generalny Inspektor nie podzielił stwierdzenia, jakoby niezasadnym byłoby kwestionowanie objęcia fotografii mianem dokumentu. Zgodnie z komentarzem do art. 76 Kodeksu postępowania administracyjnego: *„Dokumentem w znaczeniu kodeksowym jest przedmiot pokryty pismem w celu utrwalenia myśli (W. Broniewicz, Postępowanie cywilne, 1995, s. 184). (...) W sensie ścisłym dokumentem nie jest zatem plan, fotografia czy rysunek, które w rozumieniu art. 308 K.p.c. są samodzielnymi środkami dowodowymi i stosuje się do nich przepisy o dowodzie z oględzin oraz o dowodzie z dokumentu.”* (M. Jaśkowska, A. Wróbel, Kodeks postępowania administracyjnego. Komentarz., LEX 2009). W odniesieniu do kwestionowanych zapisów § 3 ust. 2 projektu rozporządzenia, Generalny Inspektor podtrzymał swoje zastrzeżenia do tej jednostki redakcyjnej w związku z treścią § 9 ust. 1 projektu. Za dyskryminujące i niezgodne z przepisami ustawy o ochronie danych osobowych uznał dołączanie do zgłoszenia o przystąpieniu do konkursu na stanowisko asystenta sędziego nieokreślonych „dokumentów potwierdzających dodatkowe kwalifikacje i osiągnięcia” kandydata w przypadku, gdy warunki zatrudnienia na stanowisku asystenta sędziego określa ustawa. Zdaniem Generalnego Inspektora nawet jeśli złożenie określonych dokumentów jest dobrowolne, projektodawca przewiduje, iż ich niespełnienie może skutkować negatywnymi konsekwencjami dla kandydata ubiegającego się o zatrudnienie na tym stanowisku, co *expressis verbis* przewiduje się w § 9 ust. 1 projektu. Dodatkowo Generalny Inspektor podkreślił, że w żaden sposób nie określa się zakresu danych osobowych przetwarzanych na tę okoliczność, co przy ustawowym uregulowaniu danej instytucji winno mieć miejsce i stanowić gwarancję przestrzegania zasad przetwarzania danych osobowych, wyrażonych w art. 26 ust. 1 pkt 1- 3 ustawy o ochronie danych osobowych. Warto wskazać, że Generalny Inspektor przyjął wyjaśnienia autora projektu odnośnie charakteru i funkcji rezerwowej listy kandydatów. Zauważył również, że w nowej wersji projektu nie

---

<sup>155</sup> DOLiS-033-168/13

<sup>156</sup> DOLiS-033-26/12/13850; rozporządzenie wydawane na podstawie art. 155a § 7 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070 z późn. zm.).



została uwzględniona uwaga zgłoszona do § 10 ust. 1 i § 12 ust. 2 projektu rozporządzenia, dotycząca postulatu stworzenia zamkniętego katalogu danych, w tym danych osobowych, przetwarzanych na okoliczność protokołu przebiegu konkursu oraz informacji o wynikach konkursu. Generalny Inspektor podkreślił również, że w żaden sposób nie odniesiono się do propozycji dotyczącej rozważenia zasadności umieszczania informacji o wynikach konkursu na stanowisko asystenta sędziego w siedzibie sądu oraz w Biuletynie Informacji Publicznej w kontekście publikowania informacji o wynikach uzyskanych przez poszczególnych kandydatów (§ 12 ust. 2 pkt 3 projektu), jak również odniesienia się do proponowanego modelu regulacji przebiegu konkursu na stanowisko asystenta sędziego, w którym informacja o kandydatach przystępujących do konkursu nie byłaby publikowana, zaś upublicznieniu podlegałyby jedynie informacja o kandydatach (imiona i nazwiska) zakwalifikowanych do zatrudnienia (§ 9 ust. 2 projektu rozporządzenia) oraz liczba kandydatów, którzy wzięli udział w postępowaniu konkursowym. Do dnia opracowania niniejszego *Sprawozdania* uwagi Generalnego Inspektora nie straciły na swej aktualności<sup>157</sup>.

Warta uwagi była również opinia Generalnego Inspektora dotycząca *projektu rozporządzenia Ministra Sprawiedliwości w sprawie przeprowadzania konkursu na stanowisko referendarza sądowego*<sup>158</sup>. Generalny Inspektor zauważył, że z punktu widzenia przepisów ustawy o ochronie danych osobowych nie mogą zyskać poparcia organu do spraw ochrony danych osobowych następujące rozwiązania zaproponowane w ww. projekcie. W § 2 ust. 2 pkt 5 projektu rozporządzenia w zakresie, w jakim jego treść odsyła do § 3 ust. 1, określenie „wymaganych dokumentów” w kontekście obowiązku złożenia przez kandydata na stanowisko referendarza sądowego 3 aktualnych fotografii (pkt 5) jest niezgodne z określeniem fotografii mianem dokumentu. Generalny Inspektor nie zgodził się ponadto z regulacjami wynikającymi z wspomnianego § 3 ust. 1 pkt 4 dotyczącego zapisu mówiącego o konieczności złożenia oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych na potrzeby konkursu na stanowisko referendarza sądowego. Analiza proponowanego zapisu prowadziła do wniosku, że jego wprowadzenie do treści rozporządzenia jest zbędne. Należy bowiem pamiętać o zasadach wynikających z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, a co za tym idzie, jeśli konkretny przepis ustawy Prawo o ustroju sądów powszechnych uprawnia lub zobowiązuje prezesa sądu do określonego działania, organ ten może przetwarzać dane osobowe w zakresie niezbędnym do wykonywania tych działań bez potrzeby wprowadzania do rozporządzenia treści proponowanej w § 3 ust. 1 pkt 4 projektu. Analizując zagadnienia związane z wyrażaniem zgody na zamieszczanie i przetwarzanie danych osobowych Generalny Inspektor wskazał, iż zgoda nie jest

---

<sup>157</sup> W aktualnym stanie prawnym projekt posiada już status obowiązującego aktu prawnego. Został on ogłoszony w Dz. U. z dnia 26 marca 2012 r. jako rozporządzenie Ministra Sprawiedliwości z dnia 16 marca 2012 r. w sprawie przeprowadzania konkursu na stanowisko asystenta sędziego (Dz. U. z 2012 r. poz. 316).

<sup>158</sup> DOLiS-033-47/12/9888; rozporządzenie wydawane na podstawie art. 149a § 2 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. Nr 98, poz. 1070 z późn. zm.).

potrzebna, gdy na danych osobowych będą dokonywane operacje w granicach obowiązujących przepisów prawa. Jeśli natomiast proces przetwarzania danych osobowych miałby dotyczyć innych sytuacji, niż przewidziane mocą tychże przepisów, to trzeba je w tym zakresie uzupełnić poprzez precyzyjne sformułowanie jakie podmioty, na jakiej podstawie i na jakich zasadach będą te dane przetwarzać. Generalny Inspektor powołał treść art. 7 pkt 5<sup>159</sup> ustawy o ochronie danych osobowych, podkreślając przy tym prawo do odwołania zgody na przetwarzanie danych osobowych, która to zgoda może być odwołana w każdym czasie. W związku z powyższym Generalny Inspektor uznał, że wprowadzenie proponowanej klauzuli zgody na zamieszczenie i przetwarzanie danych osobowych przepisami rozporządzenia wprowadziłoby problemy interpretacyjne co do prawa ewentualnego odwołania takiego oświadczenia, a w konsekwencji co do podstawy prawnej dalszego przetwarzania danych osobowych. Sprzeciw Generalnego Inspektora Ochrony Danych Osobowych budziła również treść § 3 ust. 2 projektu rozporządzenia w zakresie, w jakim przewiduje możliwość dołączenia do zgłoszenia o przystąpieniu do konkursu na stanowisko referendarza sądowego dokumentów potwierdzających dodatkowe kwalifikacje i osiągnięcia. Zdaniem Generalnego Inspektora, to z pozoru neutralne uprawnienie skutkuje bowiem negatywnymi rozstrzygnięciami dla kandydata na to stanowisko - w razie uzyskania przez kilku kandydatów tej samej liczby punktów komisja dokonuje wyboru kandydata, biorąc pod uwagę jego doświadczenie w stosowaniu prawa oraz dodatkowe kwalifikacje i osiągnięcia wynikające z dokumentów dołączonych do zgłoszenia (§ 9 ust. 1 zdanie drugie projektu rozporządzenia). W świetle ustawowego określenia instytucji prawnej referendarza sądowego (w tym wymagań dotyczących objęcia takiego stanowiska – *vide* art. 149 ustawy Prawo o ustroju sądów powszechnych), zdaniem Generalnego Inspektora wprowadzanie przepisami rozporządzenia dodatkowych, niezdefiniowanych kryteriów w postaci „*dodatkowych kwalifikacji i osiągnięć wynikających z dokumentów dołączonych do zgłoszenia*”, w tym nieokreślonych co do treści dokumentów i danych osobowych przetwarzanych na tę okoliczność, należy uznać za działanie niezgodne z prawem. Taki zapis rozporządzenia zaprzecza również celom konkursu określonym w art. 149a § 1 ustawy Prawo o ustroju sądów powszechnych, zgodnie z którymi konkurs „*ma na celu wyłonienie kandydata o największej wiedzy i najwyższych umiejętnościach, predyspozycjach i zdolnościach ogólnych*” niezbędnych do wykonywania zadań na tym stanowisku. Z punktu widzenia ochrony danych osobowych w przypadku przyjmowania rozwiązań, dla realizacji których niezbędne będzie przetwarzanie danych osobowych (to jest informacji dotyczących lub identyfikujących osoby fizyczne), należy ograniczać katalog przetwarzanych danych do niezbędnego minimum i dopuszczać przetwarzanie jedynie danych niezbędnych, koniecznych dla realizacji celów oznaczonych stosownymi

---

159 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.

przepisami prawa (art. 26 ust. 1 ustawy o ochronie danych osobowych). Takiego ograniczenia brakowało jednak w treści § 10 ust. 1 i § 12 ust. 2 projektu rozporządzenia, w których to wstęp do wyliczenia poprzedzono wyrażeniem: „w szczególności”. Wyrażenie to wprowadza otwarty i niczym nieograniczony katalog danych, w tym danych osobowych, przetwarzanych odpowiednio na okoliczność sporządzenia protokołu przebiegu konkursu oraz informacji o wynikach konkursu. Mimo iż treść § 10 ust. 1 projektu rozporządzenia reguluje zasady funkcjonowania komisji konkursowej, z punktu widzenia ujednolicania terminologii stosowanej w rozporządzeniu oraz zasad ochrony danych osobowych, Generalny Inspektor proponował takie jego przeredagowanie, aby we fragmentach odnoszących się do wskazania kandydatów określały zakres przetwarzanych danych osobowych w takiej sytuacji (np. pkt 1 proponuje się nadać brzmienie: „1) imiona i nazwiska kandydatów, którzy przystąpili do konkursu;”). W odniesieniu do § 12 ust. 1 i 2 projektu rozporządzenia Generalny Inspektor Ochrony Danych Osobowych proponował rozważenie rezygnacji z publikowania w miejscu powszechnie dostępnym w siedzibie sądu oraz w Biuletynie Informacji Publicznej imion i nazwisk kandydatów wraz z uzyskanymi przez nich wynikami w postępowaniu konkursowym w odniesieniu do tych kandydatów, którzy nie uzyskali wymaganej liczby punktów do mianowania na stanowisko referendarza sądowego. Zdaniem Generalnego Inspektora proponowane przez Ministra Sprawiedliwości rozwiązanie zobowiązujące prezesa sądu do publikacji wyników poszczególnych kandydatów, może prowadzić do naruszenia prywatności osób, które uzyskały niższą, niż wymagana w konkursie, liczbę punktów, a ich dane osobowe wraz z informacją o liczbie uzyskanych punktów byłyby mimo to dostępne dla każdego użytkownika Internetu. W kontekście obowiązków publikacyjnych nie był też jasny charakter ani funkcja pełniona przez fakultatywnie ustalaną przez komisję konkursową listę rezerwową kandydatów (jest o niej mowa w § 9 ust. 3, § 10 ust. 1 pkt 3 i § 12 ust. 1 pkt 4 projektu rozporządzenia), w kontekście zapisu § 2 ust. 2 pkt 3 projektu rozporządzenia wskazującego, iż jednym z wymogów treści ogłoszenia o konkursie na stanowisko referendarza sądowego jest określenie liczby wolnych stanowisk oraz art. 155a § 5 ustawy Prawo o ustroju sądów powszechnych. Generalny Inspektor pozostawił do decyzji projektodawcy model regulacji przebiegu konkursu na stanowisko referendarza sądowego, w którym upublicznieniu podlegałyby jedynie informacja o kandydatach (imiona i nazwiska) zakwalifikowanych do zatrudnienia (§ 9 ust. 2 projektu rozporządzenia) oraz liczba kandydatów, którzy wzięli udział w postępowaniu konkursowym. Generalny Inspektor podniósł również, że w § 12 ust. 2 opiniowanego projektu nie było jasne, czym kierował się projektodawca wskazując, iż w przypadku wyboru jednego kandydata na stanowisko referendarza sądowego publikuje się jego imię i nazwisko, a w przypadku, gdy wybrano co najmniej 2 kandydatów jest już mowa o „liście kandydatów wybranych” bez enumeratywnego wskazania, jakie dane osobowe tychże osób będą przetwarzane na potrzeby obowiązku informacyjnego. Generalny Inspektor proponował, aby w przypadku uznania zasadności ww. uwag tak przeredagować

dotychczasową treść projektu rozporządzenia, aby zapewniał on adekwatne przetwarzanie danych osobowych w stosunku do celów rozporządzenia określonych w ustawie Prawo o ustroju sądów powszechnych. Generalny Inspektor wskazał również na konieczność dokonania w projekcie rozporządzenia poprawek o charakterze legislacyjnym<sup>160</sup>.

Szczególnie wartą uwagi była też opinia Generalnego Inspektora Ochrony Danych osobowych dotycząca *projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013*<sup>161</sup>, wydawanego na podstawie art. 18 ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej (Dz. U. Nr 88, poz. 439 z późn. zm.). W pierwszej kolejności Generalny Inspektor wyraził stanowczy sprzeciw wobec – zamieszczonej na str. 471 – 474 załącznika do projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013 - propozycji badania 1.80.02(244) System Jednostek do Badań Społecznych. Biorąc pod uwagę treść art 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej, zasadnicze zastrzeżenie Generalnego Inspektora wzbudziła sama koncepcja nałożenia na: Ministerstwo Spraw Wewnętrznych, Ministerstwo Finansów, Narodowy Fundusz Zdrowia, Zakład Ubezpieczeń Społecznych, Kasę Rolniczego Ubezpieczenia Społecznego, Powiatowe Zespoły Orzekania o Niepełnosprawności, Powiatowe Urzędy Pracy, Naczelną Izbę Lekarską, Naczelną Izbę Pielęgniarek i Położnych, Krajową Izbę Diagnostów Laboratoryjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych, obowiązku przekazania Głównemu Urzędowi Statystycznemu odpowiednio: danych jednostkowych ze zbioru PESEL, danych jednostkowych dotyczących osób fizycznych z Krajowej Ewidencji Podatników, danych jednostkowych dotyczących osób fizycznych z bazy danych o podatnikach podatku dochodowego od osób fizycznych, danych jednostkowych dotyczących osób fizycznych z Centralnego Wykazu Świadczeniobiorców, danych jednostkowych dotyczących osób fizycznych z systemu emerytalno-rentowego, danych jednostkowych o osobach pobierających świadczenia rolnicze z KRUS, danych jednostkowych z Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności, rejestru bezrobotnych i poszukujących pracy, danych jednostkowych z Centralnego Rejestru Lekarzy, Centralnego Rejestru Felczerów, Centralnego Rejestru Pielęgniarek i Położnych, Rejestru Diagnostów Laboratoryjnych oraz danych jednostkowych dotyczących osób fizycznych z baz danych prowadzonych przez dostawców publicznie dostępnych usług telekomunikacyjnych. Generalny Inspektor podkreślił jednocześnie, że abstrahując nawet od faktu, iż wykonanie – wskazanych wyżej – obowiązków przez podmioty wskazane w projekcie skutkowałoby (wbrew zastrzeżeniom zgłaszanym wielokrotnie w tej kwestii przez organ do spraw ochrony danych osobowych) powstaniem w Głównym Urzędzie Statystycznym kolejnej megabazy danych

---

<sup>160</sup> W aktualnym stanie prawnym projekt posiada status obowiązującego aktu prawnego. Został ogłoszony w Dz. U. z dnia 27 marca 2012 r. jako rozporządzenia Ministra Sprawiedliwości z dnia 22 marca 2012 r. w sprawie przeprowadzania konkursu na stanowisko referendarza sądowego (Dz. U. z 2012 r. poz. 331).

<sup>161</sup> DOLiS-033-179/12/23928

(z wszystkimi negatywnymi konsekwencjami z tym związanymi), powinność udostępnienia tak wielkiej ilości danych, w tym danych szczególnie chronionych w rozumieniu art. 27 ust.1 ustawy o ochronie danych osobowych, w żadnym razie nie może wynikać z aktu prawnego o randze rozporządzenia. Nie może także umknąć uwadze, iż wśród danych, które miałyby być przekazywane Głównemu Urzędowi Statystycznemu w oparciu o unormowania projektu, znajdują się także takie, które nie należą do – zamieszczonego w art. 35 ust. 1 ustawy o statystyce publicznej – katalogu danych, które służby statystyki publicznej mogą przetwarzać (choćby informacja o stopniu orzeczonej niepełnosprawności z Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności – str. 473 załącznika do projektu). Z tych wszystkich przyczyn zawarta w projekcie propozycja badania 1.80.02(244) System Jednostek do Badań Społecznych nie zyskała akceptacji Generalnego Inspektora Ochrony Danych Osobowych. Przechodząc do badania 1.80.01(243) System Jednostek Statystycznych (str. 462 – 470 załącznika do projektu) Generalny Inspektor zakwestionował rozszerzenie zakresu danych pozyskiwanych od Zakładu Ubezpieczeń Społecznych (z Centralnego Rejestru Ubezpieczonych). Uwzględniając – statuowaną przez art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych – zasadę adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane, Generalny Inspektor nie znalazł żadnego racjonalnego uzasadnienia dla nałożenia na Zakład Ubezpieczeń Społecznych obowiązku przekazywania Głównemu Urzędowi Statystycznemu – nieprzewidzianych w obowiązującym rozporządzeniu Rady Ministrów z dnia 22 lipca 2011 roku w sprawie programu badań statystycznych statystyki publicznej na rok 2012 (Dz. U. Nr 173 poz. 1030 z późn. zm.) – numerów PESEL, informacji o obywatelstwie i adresów ubezpieczonych.

W przedmiotowej sprawie Generalny Inspektor skierował również pismo do Kancelarii Prezesa Rady Ministrów zawierające uwagi odnośnie omówionego powyżej projektu. Wskazał w nim, że w dalszym ciągu nie może zyskać akceptacji organu do spraw ochrony danych osobowych – zamieszczona na str. 475 – 478 załącznika do projektu opiniowanego rozporządzenia (wersja z lipca 2012 r.) - propozycja badania 1.80.02(243) System Jednostek do Badań Społecznych. Pomimo iż w projekcie z lipca 2012 r. Główny Urząd Statystyczny zrezygnował z pozyskiwania danych o osobach niepełnosprawnych z Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności (EKSMON), to nadal aktualne pozostały zamiary tworzenia kolejnej megabazy danych dotyczących osób fizycznych. GODO ponownie wskazał, że utworzenie przedmiotowej bazy danych miałyby nastąpić poprzez nakazanie – na mocy aktu prawnego o randze rozporządzenia – przekazania Głównemu Urzędowi Statystycznemu przez szereg instytucji państwowych, danych jednostkowych o osobach pobierających świadczenia rolnicze z KRUS z systemu informacyjnego o świadczeniobiorcach, danych jednostkowych dotyczących osób fizycznych z rejestrów bezrobotnych i poszukujących pracy, danych jednostkowych dotyczących osób fizycznych z Centralnego Rejestru

Lekarzy, Centralnego Rejestru Felczerów, Centralnego Rejestru Pielęgniarek i Położnych, Rejestru Diagnostów Laboratoryjnych oraz danych jednostkowych dotyczących osób fizycznych z baz danych prowadzonych przez dostawców publicznie dostępnych usług telekomunikacyjnych. Generalny Inspektor podkreślił, że przedłożony do zaopiniowania projekt statuuje po stronie wielu podmiotów zobowiązanych powinność udostępnienia danych Głównemu Urzędowi Statystycznemu nieznaną ustawom regulującym prowadzenie, administrowanych przez te podmioty, zbiorów danych, co stanowi naruszenie zasady hierarchiczności aktów prawnych, jak również samodzielnie kreuje prawny obowiązek o tak zasadniczym znaczeniu dla gwarantowanych konstytucyjnie praw obywateli. Z przytoczonych wyżej przyczyn Generalny Inspektor podtrzymał swoje negatywne stanowisko wobec – zawartej na str. 475 – 478 załącznika do analizowanego projektu propozycji badania 1.80.02(243) System Jednostek do Badań Społecznych, wyrażone w piśmie z dnia 13 kwietnia 2012 roku skierowanym do Prezesa Głównego Urzędu Statystycznego. W odniesieniu zaś do badania 1.80.01(242) System Jednostek Statystycznych (str. 466 – 474 załącznika do projektu z lipca 2012 r.) zakwestionowane zostało rozszerzenie zakresu danych pozyskiwanych od Zakładu Ubezpieczeń Społecznych (z Centralnego Rejestru Ubezpieczonych). Uwzględniając – statuuowaną 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 nie znalazł żadnego uzasadnienia dla nałożenia na Zakład Ubezpieczeń Społecznych obowiązku przekazywania Głównemu Urzędowi Statystycznemu numerów PESEL, informacji o obywatelstwie i adresów ubezpieczonych (nieprzewidzianych w obowiązującym rozporządzeniu Rady Ministrów z dnia 22 lipca 2011 roku w sprawie programu badań statystycznych statystyki publicznej na rok 2012 – Dz. U. Nr 173, poz. 1030 z późn. zm.). W związku z przewidzianym w badaniu 1.29.02(084) Zachorowania i leczenia na wybrane choroby (str. 186 – 190 załącznika do projektu z lipca 2012 r.) obowiązkiem przekazywania danych do regionalnych rejestrów onkologicznych i Krajowego Rejestru Chorób Nowotworowych, organ do spraw ochrony danych osobowych po raz kolejny (kwestia ta była już przedmiotem pism z dnia 25 kwietnia 2012 roku i z dnia 28 maja 2012 roku skierowanych do Prezesa Głównego Urzędu Statystycznego) zwrócił uwagę na fakt, iż – w myśl art. 53<sup>162</sup> ustawy z dnia

---

<sup>162</sup> Art. 53. 1. Podmiot prowadzący do dnia wejścia w życie niniejszej ustawy rejestry, ewidencje, listy, spisy albo inne uporządkowane zbiory danych osobowych lub jednostkowych danych medycznych, w zakresie określonym w art. 19 ust. 1, w terminie 6 miesięcy od dnia wejścia w życie ustawy, jest obowiązany przekazać ministrowi właściwemu do spraw zdrowia informacje o ich prowadzeniu oraz zakresie danych w nich zawartych. 2. Informacje, o których mowa w ust. 1, są przekazywane za pośrednictwem jednostki podległej ministrowi właściwemu do spraw zdrowia, właściwej w zakresie systemów informacyjnych ochrony zdrowia. Jednostka ta weryfikuje przekazane informacje oraz przedstawia ministrowi właściwemu do spraw zdrowia analizę potrzeb utworzenia rejestru medycznego, o której mowa w art. 19 ust. 3 i 4. 3. W przypadku stwierdzenia zasadności utworzenia rejestru medycznego, minister właściwy do spraw zdrowia, w terminie 6 miesięcy od dnia upływu terminu, o którym mowa w ust. 1, tworzy ten rejestr w sposób określony w art. 20 ust. 1. 4. W terminie 6 miesięcy od dnia utworzenia rejestru w sposób określony w art. 20 ust. 1, podmiot prowadzący rejestr jest obowiązany przekazać każdej osobie, której dane są przetwarzane w tym rejestrze, informacje określone w art. 19 ust. 9. 5. Podmiot prowadzący do dnia wejścia w życie niniejszej ustawy rejestry, ewidencje, listy, spisy albo inne uporządkowane zbiory danych osobowych lub jednostkowych danych medycznych, w zakresie określonym w art. 19 ust. 1, w przypadku których, w terminie określonym w ust. 3, nie utworzono rejestru medycznego w sposób określony w art. 20 ust. 1, jest obowiązany w terminie miesiąca od dnia upływu terminu, o którym mowa w ust. 3, do zaprzestania ich prowadzenia oraz zniszczenia baz danych i

28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 z późn. zm.) brak jest w obecnym stanie prawnym podstawy dla prowadzenia w 2013 roku tych rejestrów onkologicznych. Biorąc pod uwagę, że rozporządzenie, o którym stanowi ww. art. 53 ustawy o systemie informacji w ochronie zdrowia nie zostało dotychczas wydane, brak jest podstaw prawnych dla prowadzenia regionalnych rejestrów onkologicznych i Krajowego Rejestru Chorób Nowotworowych po dniu 31 grudnia 2012 roku - a zatem po tej dacie dane do tych rejestrów nie będą mogły być przekazywane.

W kolejnym piśmie kierowanym do Prezesa GUS w dniu 10 września 2012 roku, Generalny Inspektor poinformował, iż wzgląd na – statuowaną w art. 7 Konstytucji Rzeczypospolitej Polskiej oraz w art. 26 ustawy o ochronie danych osobowych - zasadę legalizmu nie pozwala organowi do spraw ochrony danych osobowych na zaakceptowanie propozycji Prezesa Głównego Urzędu Statystycznego w przedmiocie uznania za uzgodnione projektów: rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013 i rozporządzenia Prezesa Rady Ministrów w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2013. Generalny Inspektor wskazał, że pierwsze przekazanie za pomocą formularza statystycznego „MZ/N-1a – karta zgłoszenia nowotworu złośliwego” na potrzeby badania 1.29.02(084) – Zachorowania i leczenia na wybrane choroby, danych osób dotkniętych chorobami nowotworowymi miało nastąpić w terminie do dnia 15 stycznia 2013 roku. Tymczasem – jak zostało to już wykazane we wcześniejszych pismach Generalnego Inspektora Ochrony Danych Osobowych (z dnia 25 kwietnia 2012 r. i z dnia 28 maja 2012 r.) z dniem 31 grudnia 2012 roku wygasła podstawa prawna dla prowadzenia Krajowego Rejestru Chorób Nowotworowych i regionalnych rejestrów onkologicznych. Tym samym od dnia 1 stycznia 2013 roku w istocie bezprzedmiotowy stał się – proponowany w pkt 26 – 27 projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013 – obowiązek przekazywania danych do tych rejestrów. Generalny Inspektor poinformował, że z uwagi na powyższe zaproponowana konstrukcja prawna polegająca na wpisaniu do projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013 (pkt 26 – 27) obowiązku przekazywania danych do Krajowego Rejestru Chorób Nowotworowych i regionalnych rejestrów onkologicznych w oparciu o założenie, że do dnia 1 stycznia 2013 roku zacznie obowiązywać rozporządzenie Ministra Zdrowia legalizujące prowadzenie tych rejestrów w 2013 roku (czyli niejako

---

nośników informacji w sposób uniemożliwiający ich wykorzystanie, chyba że rejestry, ewidencje, listy, spisy albo inne uporządkowane zbiory danych osobowych lub jednostkowych danych medycznych stanowią materiały archiwalne w rozumieniu przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, co potwierdza dyrektor właściwego archiwum państwowego w trybie, określonym w przepisach art. 5 ust. 2 i 2b tej ustawy. 6. O okolicznościach określonych w ust. 5 podmiot powiadamia pisemnie ministra właściwego do spraw zdrowia oraz jednostkę podległą ministrowi właściwemu do spraw zdrowia, właściwą w zakresie systemów informacyjnych ochrony zdrowia.

warunkowo), nie wydaje się prawidłowa. Konstrukcja taka, w wypadku jej przyjęcia, prowadziłaby do zaistnienia poważnych problemów prawnych, gdyby jednak stosowne rozporządzenie Ministra Zdrowia nie zaczęło we wskazanym wyżej terminie obowiązywać. Biorąc również pod uwagę, iż przedmiotowe zagadnienie dotyczyło przetwarzania danych o stanie zdrowia, czyli danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych ponownie podkreślił, że nie może zgodzić się z przedłożoną propozycją i podtrzymał swoje zastrzeżenia do projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013, zawarte zarówno w piśmie do Prezesa GUS z dnia 13 kwietnia 2012 roku, jak i w piśmie skierowanym do Podsekretarza Stanu w Kancelarii Prezesa Rady Ministrów, Zastępcy Przewodniczącego stałego komitetu Rady Ministrów z dnia 16 sierpnia 2012 roku. Marginesowo zauważył przy tym, że dotychczas nie zostały także rozstrzygnięte wątpliwości organu do spraw ochrony danych osobowych zgłoszone wobec propozycji badania 1.80.02(243) – System Jednostek do Badań Społecznych (str. 475– 478 załącznika do projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013)<sup>163</sup>.

Dodatkowo wskazać można, że Rada Legislacyjna przy Prezesie Rady Ministrów podzieliła wątpliwości, które Generalny Inspektor wyrażał w kwestii zasad pozyskiwania przez służby statystyki publicznej danych od podmiotów zobowiązanych do wypełniania obowiązku statystycznego (pismo z dnia 14 września 2012 r., znak: RL-0303-19/12).

Powiązana z omówionym powyżej projektem była opinia Generalnego Inspektora dotycząca *rozporządzenia Prezesa Rady Ministrów w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2012*<sup>164</sup>. Zastrzeżenia GODO wzbudził formularz statystyczny „MZ/N-1a – karta zgłoszenia nowotworu złośliwego”, w którym zauważył, że – zgodnie z projektem rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013 (§ 2 projektu oraz str. 187 załącznika do projektu) – formularz ten ma być wykorzystywany w 2013 roku (pkt 26 badania 1.29.02(085) – Zachorowania i leczeni na wybrane choroby) oraz w okresie do 30 czerwca 2014 roku (pkt 27 badania 1.29.02(085) – Zachorowania i leczeni na wybrane choroby) i do 15 grudnia 2014 roku (pkt 28 badania 1.29.02(085) – Zachorowania i leczeni na wybrane choroby) – z danymi za rok 2013. Tymczasem w myśl art. 53 ustawy o systemie informacji w ochronie zdrowia brak było podstawy dla prowadzenia w 2013 roku rejestrów onkologicznych, o których mowa w pkt 26

---

<sup>163</sup> Projekt posiada status obowiązującego aktu prawnego – został on ogłoszony w Dz. U. z dnia 12 grudnia 2012 r. jako rozporządzenie Rady Ministrów z dnia 9 listopada 2012 r. w sprawie programu badań statystycznych statystyki publicznej (Dz. U. z 2012 r. poz. 1391).

<sup>164</sup> DOLiS-033-197/12/25980



– 28 projektu rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013. Generalny Inspektor ponownie powołał art. 53 ustawy o systemie informacji w ochronie zdrowia i określił, że rozporządzenie o którym stanowi ww. przepis nie zostało dotychczas wydane i co za tym idzie - uprawnienie ustawowe dla prowadzenia wskazanych wyżej rejestrów onkologicznych, wygasa z dniem 31 grudnia 2012 roku. W związku z powyższym w 2013 roku kwestionowany przez Generalnego Inspektora Ochrony Danych Osobowych formularz statystyczny „MZ/N-1a – karta zgłoszenia nowotworu złośliwego” nie będzie mógł być stosowany.

W kolejnym piśmie dotyczącym przedmiotowego rozporządzenia Generalny Inspektor wskazał, że nie może – niestety – zaakceptować propozycji Prezesa Głównego Urzędu Statystycznego w przedmiocie uznania za uzgodniony, projektu rozporządzenia Prezesa Rady Ministrów w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2013 (wersja z dnia 14.03.2012 r. przesłana do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych pismem Prezesa Głównego Urzędu Statystycznego z dnia 5 kwietnia 2012 roku). Generalny Inspektor nie mógł bowiem pominąć, że kwestia braku podstawy prawnej dla pozyskiwania przez Ministerstwo Zdrowia (i podległe mu jednostki organizacyjne) danych osób dotkniętych nowotworami była zawsze przedmiotem szczególnej uwagi organu do spraw ochrony danych osobowych. Poczynając od 2006 roku GODO był informowany o toczących się w Ministerstwie Zdrowia intensywnych pracach zmierzających do prawidłowego i całościowego unormowania tego zagadnienia. To wieloletnie doświadczenie nastawiło sceptycznie organ do spraw ochrony danych osobowych co do terminowego, do 31 grudnia 2012 roku – art. 53 ust. 3 w zw. z ust. 1 i art. 58 ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 z późn. zm.) – wywiązania się przez Ministerstwo Zdrowia z obowiązku wydania rozporządzenia dotyczącego prowadzenia rejestru zachorowań na nowotwory złośliwe. Z uwagi na to, że kwestionowany przez GODO formularz statystyczny „MZ/N-1a – karta zgłoszenia nowotworu złośliwego” miał być wykorzystywany w 2013 roku, z drugiej zaś strony nie był mu znany choćby wstępny projekt wskazanego w piśmie Prezesa GUS rozporządzenia Ministra Zdrowia dotyczącego prowadzenia rejestru zachorowań na nowotwory złośliwe, Generalny Inspektor Ochrony Danych Osobowych podtrzymał swoje uwagi zawarte w piśmie z dnia 25 kwietnia 2012 r.

W ramach *projektu rozporządzenia Prezesa Rady Ministrów w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2013*, Generalny Inspektor opiniował również szereg formularzy w zakresie: „SSI-01 – sprawozdanie o wykorzystaniu technologii

informacyjno-telekomunikacyjnych w przedsiębiorstwach”, „SSI-02 – sprawozdanie o wykorzystaniu technologii informacyjno-telekomunikacyjnych w przedsiębiorstwach sektora finansowego”, „ZD-2 – sprawozdanie z lecznictwa uzdrowiskowego, stacjonarnych zakładów rehabilitacji leczniczej za 2013 r.”, „ZD-3 – sprawozdanie z ambulatoryjnej opieki zdrowotnej za 2013 r.”, „ZD-4 – sprawozdanie z pomocy doraźnej i ratownictwa medycznego za 2013 r.”, „DS-51G – turystyka i wypoczynek w gospodarstwach domowych, kwestionariusz gospodarstwa domowego”, „DS-51I – turystyka i wypoczynek w gospodarstwach domowych, kwestionariusz indywidualny wyjazdu”, „SSI-10G – wykorzystanie technologii informacyjno-telekomunikacyjnych w gospodarstwach domowych. Kwestionariusz dla gospodarstwa domowego”, „NBP-NK – ankieta dotycząca nieruchomości komercyjnych”, „SG-01 – statystyka gminy: samorząd i transport za 2013 rok”, „ST-P – statystyka powiatu: samorząd i transport za 2013 rok” i „ST-W – statystyka województwa: samorząd i transport za 2013 rok”, w ramach których nie zgłosił uwag. Niemniej jednak sprzeciw Generalnego Inspektora wzbudziła propozycja brzmienia działu X. CHARAKTERYSTYKA OSOBY formularza „SSI-10I – wykorzystanie technologii informacyjno-telekomunikacyjnych w gospodarstwach domowych. Kwestionariusz indywidualny”. Generalny Inspektor wskazał, że z nieznanego dla niego powodów, w tej części formularza statystycznego, dotyczącego przecież wykorzystania technologii informacyjno-telekomunikacyjnych w gospodarstwie domowym, znalazły się pytania o: pozostawaniu przez respondenta w związku partnerskim (pkt 6 działu X.) i orzeczonej niepełnosprawności respondenta (pkt 8 działu X.), fakcie ewentualnego korzystania przez respondenta z pomocy społecznej (pkt 9 działu X.). Abstrahując już od – zdawać by się mogło – oczywistego braku związku tych pytań z przedmiotem badania, trudno było wskazać jakiejkolwiek przyczyny, dla których służby statystyki publicznej miałyby pozyskiwać tego rodzaju informacje, należące przecież do najintymniejszej sfery życia prywatnego i rodzinnego osoby fizycznej, uzyskując je niejako „przy okazji” prowadzonego badania statystycznego. Generalny Inspektor podkreślił, że takie zachowanie służb statystyki publicznej stanowiłoby naruszenie – gwarantowanego przez Konstytucję Rzeczypospolitej Polskiej – prawa osoby fizycznej do prywatności (art. 47) i ochrony dotyczących jej danych osobowych (art. 51), jak również – statuowanych w art. 26 ust. 1 pkt 1 i pkt 3 ustawy o ochronie danych osobowych – zasad legalizmu i adekwatności przetwarzanych danych w stosunku do celów, w jakich są one przetwarzane. Generalny Inspektor wskazał również, że pozyskiwanie danych tego rodzaju przez służby statystyki publicznej wykracza poza zakres ich upoważnienia do przetwarzania danych osób fizycznych określonego w art. 35 ust. 1 ustawy o statystyce publicznej. Okoliczność, iż art. 35 ust. 1 pkt 6 ustawy o statystyce publicznej dopuszcza dla celów statystycznych i przygotowania prognoz demograficznych zbieranie informacji o datach zawarcia i ustania małżeństw, nie jest równoznaczna z prawem służb statystyki publicznej do pozyskiwania tego typu informacji dla związków partnerskich (wobec nieuchwalenia ustawy o związkach partnerskich prawo polskie w ogóle nie zna takiego pojęcia). W odniesieniu do

informacji o niepełnosprawności i korzystaniu z pomocy społecznej, Generalny Inspektor przypomniał, że są to dane szczególnie chronione w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, których przetwarzanie, bez pisemnej zgody osób, których dotyczą, wymaga przepisu szczególnego rangi ustawowej, stwarzającego pełne gwarancje ochrony takich danych (art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych). W związku z powyższym Generalny Inspektor uznał, że regulacja zawarta w rozporządzeniu nie może być uznana za wystarczającą dla legalnego przetwarzania danych tego rodzaju przez służby statystyki publicznej.

Generalny Inspektor wskazał swoje negatywne stanowisko wobec proponowanego brzmienia formularza „SSI-10I – wykorzystanie technologii informacyjno-telekomunikacyjnych w gospodarstwach domowych. Kwestionariusz indywidualny”, który miał zostać włączony do projektu rozporządzenia Prezesa Rady Ministrów w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2013. O ile fakt dobrowolności udziału w badaniu nie może pozostawać bez wpływu na ocenę dopuszczalności pozyskiwania za pomocą analizowanego formularza określonych informacji, to nie można jednocześnie pominąć, iż dobrowolność taka nie konwaliduje gromadzenia danych w zakresie szerszym, aniżeli dopuszczony przez przepisy prawa, czy też danych nieadekwatnych. Zdaniem GODO rozporządzenie Komisji (UE) nr 937/2011 z dnia 21 września 2011 r. w sprawie wykonania rozporządzenia (WE) nr 808/2004 Parlamentu Europejskiego i Rady dotyczącego statystyk Wspólnoty w sprawie społeczeństwa informacyjnego – Dz. Urz. UE L 245 z 22.09.2011, str. 1 – w załączniku II module 2 pkt 4 lit. b tiret czwarte i tiret piąte, nie nakłada obowiązku gromadzenia przez służby statystyczne informacji o stanie cywilnym (prawnym i faktycznym) osób indywidualnych objętych badaniem dotyczącym wykorzystania technologii informacyjno-telekomunikacyjnych w gospodarstwach domowych, a jedynie przewiduje taką możliwość. W związku z tym Generalny Inspektor stwierdził, że unormowania ww. rozporządzenia Komisji (UE) nr 937/2011 z dnia 21 września 2011 r. w sprawie wykonania rozporządzenia (WE) nr 808/2004 Parlamentu Europejskiego i Rady dotyczącego statystyk Wspólnoty w sprawie społeczeństwa informacyjnego, nie stanowią przepisów prawa w rozumieniu art. 23 ust. 1 pkt 2 i art. 27 ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, legalizujących pozyskiwanie przez Główny Urząd Statystyczny danych tego rodzaju. Generalny Inspektor zauważył jednocześnie, że niespornym pozostaje, iż w odniesieniu do informacji o stanie cywilnym prawnym (małżeństwach) taką przesłanką legalizującą dla Głównego Urzędu Statystycznego jest art. 35 ust. 1 pkt 6 ustawy o statystyce publicznej. Generalny Inspektor podkreślił także, że przepis ten nie może znaleźć zastosowania w przypadku przedłożonej do zaopiniowania propozycji gromadzenia przez Główny Urząd Statystyczny informacji o związkach partnerskich, gdyż w prawie polskim pojęcie to (jak dotychczas)

w ogóle nie występuje. Co więcej, Generalny Inspektor Ochrony Danych Osobowych nie dopatrywał się związku pomiędzy przedmiotem badania: „wykorzystanie technologii informacyjno-telekomunikacyjnych w gospodarstwach domowych” a przewidzianym w dziale X pkt 6 omawianego formularza zbieraniem informacji ze sfery życia prywatnego, czy wręcz seksualnego, respondentów. Generalny Inspektor stanął na stanowisku, iż żadne badanie statystyczne nie może jednocześnie stanowić pretekstu dla wkroczenia w prywatność obywateli w zakresie, czy też dziedzinach, niepozostających w bezpośrednim związku z przedmiotem tego badania. W opinii GODO taki zaś przypadek miał miejsce w odniesieniu do działu X pkt 6 formularza „SSI-10I – wykorzystanie technologii informacyjno-telekomunikacyjnych w gospodarstwach domowych. Kwestionariusz indywidualny” i dlatego oponował przeciwko temu unormowaniu. Względ na interes służb statystyki publicznej w pozyskiwaniu informacji o członkach społeczeństwa w jak najszerszym zakresie nie może bowiem przeważać nad – gwarantowanymi przez Konstytucję Rzeczypospolitej Polskiej – prawami osoby fizycznej do prywatności (art. 47) i ochrony dotyczących jej danych osobowych (art. 51). Negatywnego stanowiska Generalnego Inspektora wobec tego projektu nie zmieniła nawet proponowana zamiana sformułowania „w związku partnerskim” na sformułowanie „w związku nieformalnym”. Generalny Inspektor ocenił, że zmiana taka sprowadzałaby się w istocie do kwestii użytej terminologii i nie odnosiłaby się do meritum zagadnienia, czyli braku uprawnienia Głównego Urzędu Statystycznego do pozyskiwania informacji tego rodzaju. Wobec wyjaśnienia przyczyn uzasadniających zbieranie przez Główny Urząd Statystyczny danych o niepełnosprawności i korzystaniu przez respondentów z pomocy społecznej, a także biorąc pod uwagę – wynikającą z § 1 ust. 2 projektu rozporządzenia Prezesa Rady Ministrów w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2013, Generalny Inspektor Ochrony Danych Osobowych uznał argumenty Prezesa GUS i nie podtrzymał uwag zgłoszonych w kwestii pozyskiwania w badaniach statystycznych informacji o niepełnosprawności i o korzystaniu przez respondenta z pomocy opieki społecznej<sup>165</sup>.

Niezwykle istotnym w okresie sprawozdawczym było *wystąpienie Generalnego Inspektora do Premiera RP w związku z zastrzeżeniami zgłaszanymi organowi do spraw ochrony danych osobowych przez podmioty objęte – wynikającym z ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej (Dz. U. Nr 88, poz. 439 z późn. zm.) – obowiązkiem udostępniania danych służbom*

---

<sup>165</sup> Projekt posiada status obowiązującego aktu prawnego – został on ogłoszony w Dz. U. z dnia 25 kwietnia 2012 r. jako rozporządzenie Prezesa Rady Ministrów z dnia 7 marca 2012 r. w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystyki publicznej na rok 2012 (Dz. U. z 2012 r. poz. 446).

*statystyki publicznej*<sup>166</sup>. W oparciu o przeprowadzoną analizę przepisów tej ustawy, Generalny Inspektor przedstawił Premierowi wątpliwości odnośnie prawidłowości obowiązujących unormowań dotyczących obowiązku przekazywania danych dla celów statystyki publicznej. Najprawdopodobniej w związku z faktem, iż przepisy z zakresu statystyki publicznej zostały – w swej zasadniczej postaci – sformułowane przed wejściem w życie Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, nie korespondują one ze standardami wynikającymi z rozdziału III Konstytucji Rzeczypospolitej Polskiej, zwłaszcza dotyczącymi hierarchii źródeł prawa i zakresu materii, która może podlegać unormowaniu w przepisach podustawowych (wykonawczych). Generalny Inspektor przypomniał, że Trybunał Konstytucyjny w uzasadnieniu postanowienia z dnia 31 stycznia 2007 roku (S 1/2007) stwierdził, iż: *„Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować” funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. [...] Także art. 31 ust. 3 Konstytucji wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki. W takim wypadku zakres materii pozostawianych do unormowania w rozporządzeniu musi być węższy niż zakres materii ogólnie dozwolony na tle art. 92 ust. 1 Konstytucji. Artykuł 31 ust. 3 Konstytucji silniej bowiem akcentuje konieczność szerszego unormowania rangi ustawowej i zawęża pole regulacyjne pozostające dla rozporządzenia”*. Wbrew zaprezentowanemu stanowisku Trybunału Konstytucyjnego, ustawodawca w art. 13 ust. 3 ustawy o statystyce publicznej, statuuje obowiązek organów administracji rządowej i jednostek samorządu terytorialnego, innych instytucji rządowych, organów prowadzących urzędowe rejestry i Narodowego Banku Polskiego nieodpłatnego przekazywania służbom statystyki publicznej zgromadzonych tzw. „danych administracyjnych” (definicję tego pojęcia zawiera art. 13 ust. 1 ustawy o statystyce publicznej), określił, że zakres, forma i terminy przekazywania tych danych będą każdorazowo określone w programie badań statystycznych statystyki publicznej. Jeśli zważyć, że – w myśl art. 18 ustawy o statystyce publicznej – program badań statystycznych statystyki publicznej jest ustalany przez Radę Ministrów w drodze rozporządzenia, to nie może już ulegać wątpliwości, że to organ władzy wykonawczej, a nie ustawodawczej, w sposób wiążący rozstrzyga obecnie, jakie podmioty są zobligowane do przekazywania danych służbom statystyki publicznej i jakie dane będą przekazywane. Podobnie zagadnienie to reguluje art. 5 ust. 1 ustawy o statystyce publicznej, zgodnie z którym program badań statystycznych statystyki publicznej określa źródła, z których służby te mogą legalnie zbierać dane, w tym dane o osobach fizycznych

---

<sup>166</sup> DOLiS-033-298/12/36852

dotyczące ich życia (art. 5 ust. 1 *in fine* ustawy o statystyce publicznej), oraz art. 7 ust. 1 ustawy o statystyce publicznej, stosownie do którego w programie badań statystycznych statystyki publicznej na określony podmiot może być nałożony obowiązek przekazania danych służbom statystyki publicznej. Zdaniem Generalnego Inspektora, w świetle zaprezentowanych wyżej unormowań uzasadniona jest teza, iż w ustawie o statystyce publicznej został jedynie ukonstytuowany ogólny obowiązek statystyczny, zaś wszelkie szczegółowe regulacje konkretyzujące ten obowiązek co do jego zakresu, w tym zakresu danych podlegających przetwarzaniu dla celów statystyki publicznej, pozostawione zostały do unormowania w wydawanym corocznie rozporządzeniu – programie badań statystycznych statystyki publicznej. Takie ukształtowanie przepisów dotyczących statystyki publicznej, umożliwiające pozyskiwanie przez służby statystyki publicznej, bez kontroli Parlamentu, w istocie dowolnych danych (zgodnie bowiem z art. 35 ust. 2 zdanie drugie ustawy o statystyce publicznej zakres i formę zbierania danych osobowych niezbędnych do danego badania określa każdorazowo program badań statystycznych statystyki publicznej), pozostaje – w ocenie organu do spraw ochrony danych osobowych – w oczywistej sprzeczności z art. 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej („Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby”) oraz art. 47 w zw. z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej (ograniczenie konstytucyjnego prawa do ochrony życia prywatnego może być ustanowione tylko w ustawie i tylko wtedy, gdy jest to konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób). Generalny Inspektor nie mógł również powinąć tego, że – powoływana już wyżej w niniejszym piśmie – zasada hierarchii źródeł prawa, wyklucza dopuszczalność takiego sformułowania przepisów ustawowych, by upoważniały one do samodzielnego i wyczerpującego uregulowania w rozporządzeniu (rozporządzeniach) całego kompleksu zagadnień dotyczących określonych praw i obowiązków. Tymczasem właśnie z taką sytuacją mamy do czynienia w przypadku obowiązującej ustawy o statystyce publicznej. Wobec zasygnalizowanych problemów natury legislacyjnej, które powodować mogą naruszenia w konstytucyjnie chronionej sferze praw i wolności obywatelskich, należy zwrócić uwagę na potrzebę odniesienia się przez ustawodawcę, w ustawie o statystyce publicznej, nie tylko do zakresu zbieranych danych osobowych, ale także przynajmniej do takich – nierozstrzygniętych obecnie na jej gruncie – zagadnień, jak: forma i tryb przekazywania danych służbom statystyki publicznej, czy też okres retencji danych (w tym okresy przechowywania i usuwania danych ze zbiorów prowadzonych przez te służby). Co więcej, według Generalnego Inspektora, te wysoce kontrowersyjne przepisy regulujące przetwarzanie danych przez służby statystyki publicznej mają negatywny wpływ na całą problematykę ochrony danych osobowych. Z jednej strony bowiem rodzą one pokusę tworzenia przez te służby, w oparciu o unormowania zamieszczone w rozporządzeniach – programach badań statystycznych statystyki publicznej, megabaz

danych stanowiących poważne zagrożenie dla prawa osób fizycznych do ochrony dotyczących ich danych osobowych. Dowodem, że nie jest to zarzut bezpodstawny stanowi omówione wcześniej jako projekt, ale aktualnie już obowiązujące, rozporządzenie Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2013. W dokumencie tym Główny Urząd Statystyczny przewidział nałożenie na: Ministerstwo Spraw Wewnętrznych, Ministerstwo Finansów, Narodowy Fundusz Zdrowia, Zakład Ubezpieczeń Społecznych, Kasę Rolniczego Ubezpieczenia Społecznego, Powiatowe Zespoły Orzekania o Niepełnosprawności, Powiatowe Urzędy Pracy, Naczelną Izbę Lekarską, Naczelną Izbę Pielęgniarek i Położnych, Krajową Izbę Diagnostów Laboratoryjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych, obowiązku przekazania Głównemu Urzędowi Statystycznemu odpowiednio: danych jednostkowych ze zbioru PESEL, danych jednostkowych dotyczących osób fizycznych z Krajowej Ewidencji Podatników, danych jednostkowych dotyczących osób fizycznych z Bazy danych o podatnikach podatku dochodowego od osób fizycznych, danych jednostkowych dotyczących osób fizycznych z Centralnego Wykazu Świadczeniobiorców, danych jednostkowych dotyczących osób fizycznych z systemu emerytalno-rentowego, danych jednostkowych o osobach pobierających świadczenia rolnicze z KRUS, danych jednostkowych z Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności, rejestru bezrobotnych i poszukujących pracy, danych jednostkowych z Centralnego Rejestru Lekarzy, Centralnego Rejestru Felczerów, Centralnego Rejestru Pielęgniarek i Położnych, Rejestru Diagnostów Laboratoryjnych oraz danych jednostkowych dotyczących osób fizycznych z baz danych prowadzonych przez dostawców publicznie dostępnych usług telekomunikacyjnych. Z drugiej zaś strony do organu do spraw ochrony danych osobowych wpływają sygnały od podmiotów, że zachodzi kolizja między – zamieszczonymi w rozporządzeniach – programach badań statystycznych statystyki publicznej – unormowaniami nakładającymi na te podmioty obowiązek udostępniania danych służbom statystyki publicznej a przepisami ustaw (regulującymi zasady funkcjonowania tych podmiotów), które uzależniają dopuszczalność udostępnienia przez nie danych od istnienia w tym zakresie stosownego nakazu w przepisach rangi ustawowej. W obowiązującym stanie prawnym kolizji tej nie sposób prawidłowo rozstrzygnąć, a tym samym podmiot, którego ona dotyczy, nie wie jak prawidłowo ma się zachować w sytuacji, gdy obowiązek przekazania danych służbom statystyki publicznej wynika wprawdzie z aktu o randze ustawy (ustawy o statystyce publicznej), jednakże konkretyzacja tego obowiązku, która w istocie decyduje o tym, jak ma postępować i jakie dane udostępnić, podmiot zobowiązany znajduje już tylko w przepisie wykonawczym (rozporządzeniu w sprawie programu badań statystycznych statystyki publicznej na dany rok). Generalny Inspektor Ochrony Danych Osobowych stanął na stanowisku, iż ustawa o statystyce publicznej, ukształtowana (w zakresie najistotniejszych unormowań) jeszcze w porządku konstytucyjnym wynikającym z art. 54 ust. 1 i art. 55 ust. 3 ustawy konstytucyjnej z dnia 17 października 1992 roku o wzajemnych stosunkach między

władzą ustawodawczą i wykonawczą Rzeczypospolitej Polskiej oraz o samorządzie terytorialnym (Dz. U. Nr 84, poz. 426 z późn. zm.), nie jest już obecnie aktem prawnym prawidłowo normującym kwestie pozyskiwania danych przez służby statystyki publicznej. Dlatego też wyraził konieczność podjęcia działań legislacyjnych zmierzających do jej dostosowania do standardów wynikających z art. 92 ust. 1 Konstytucji Rzeczypospolitej Polskiej.

Wystąpienie niniejsze spotkało się z reakcją ze strony Rządowego Centrum Legislacji, które w piśmie z dnia 10 sierpnia 2012 r. (znak: RCL.DPŚiL.5602-84/12) przekazało GIODO *Analizę regulacji dotyczącą zbierania danych osobowych zawartych w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej* (Dz. U. z 2012 r. poz. 591), informując jednocześnie, iż zwróciło się z prośbą o wyrażenie przez Radę Legislacyjną opinii, czy przepisy ustawy o statystyce publicznej, które przewidują przetwarzanie danych osobowych określanych w wydawanym corocznie przez Radę Ministrów, w drodze rozporządzenia, programie badań statystyki publicznej, budzą istotne zastrzeżenia w kontekście przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Rada Legislacyjna wyraziła swój pogląd w – powoływanej wyżej – opinii dotyczącej kwestii przetwarzania danych osobowych określanych w programie badań statystyki publicznej na rok 2013<sup>167</sup>.

Wartą wskazania w niniejszym *Sprawozdaniu* była również opinia Generalnego Inspektora na temat *rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej w sprawie sposobu, trybu oraz warunków technicznych gromadzenia, przetwarzania, udostępniania i usuwania przez Głównego Inspektora Transportu Drogowego utwalonych obrazów i danych*<sup>168</sup>, wydawanego na podstawie art. 129g ust. 4 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2005 r. Nr 108, poz. 908 z późn. zm.). Generalny Inspektor poinformował, iż z punktu widzenia przepisów ustawy o ochronie danych osobowych jego aprobaty nie mogą zyskać rozwiązania przyjęte w przedmiotowym projekcie. Jak zauważył Generalny Inspektor, zgodnie ze stwierdzeniem autora pisma przewodniego, uzasadnieniem skierowania opiniowanego projektu po raz kolejny do uzgodnień międzyresortowych było wejście w życie rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526) – w dacie Komisji Prawniczej, 21 lipca 2001 r. rozporządzenie to nie miało statusu obowiązującego. Zdaniem Generalnego Inspektora taki argument wydawał się jednak wymagać dodatkowych wyjaśnień i uzupełnienia w uzasadnieniu projektu. Generalny Inspektor wskazał, że z treści delegacji do wydania opiniowanego aktu prawnego wynika, iż prawodawca upoważnił ministra właściwego do spraw transportu do określenia w drodze rozporządzenia sposobu,

---

<sup>167</sup> Pismo z dnia 14 września 2012 r. znak: RL-0303-19/12.

<sup>168</sup> DOLiS- 033-297/12/ 39390



trybu oraz warunków technicznych gromadzenia, przetwarzania i usuwania utrwalonych obrazów i danych. Nadmieniał również, że tym większa jego wątpliwość zachodzi w kontekście powołania w treści opiniowanego rozporządzenia odesłań do rozporządzenia Rady Ministrów (np. § 3 ust. 2, § 4 ust. 1 czy § 5 ust. 1 projektu), bez omówienia, jaki zakres spraw reguluje wspomniane już rozporządzenie Rady Ministrów, a jakie projektowane rozporządzenie. Z punktu widzenia poprawności legislacyjnej, zakresu spraw regulowanych owym memorandum i związku z opiniowanym rozporządzeniem, wątpliwości Generalnego Inspektora wzbudziła definicja RFC użyta w § 2 pkt 4 projektu. Odwołuje się ona bowiem do „memorandum związanych z Internetem oraz sieciami komputerowymi”. Nie jest również znana forma, ani funkcja podmiotu określanego jako Internet Engineering Task Force. Generalny Inspektor zaznaczył, że projektodawca nie rozstrzyga kwestii roli składnic danych (§ 2 pkt 2 projektu), jak również nie wyjaśnia, czy w składnicach danych pozostawia się dane po zakończeniu przez nie określonego etapu pracy. Projektodawca posłużył się jedynie enigmatycznym stwierdzeniem „Ze składnic danych sporządza się kopie zapasowe i archiwalne” - § 6 ust. 3 projektu. Wspomniał również, iż ustawa Prawo o ruchu drogowym nie posługuje się określeniem „składnica danych” w odniesieniu do urządzeń rejestrujących. W § 2 pkt 6 projektu, w odniesieniu do definicji IPsec nie przedstawiono definicji sieci prywatnej. Również wyrażenie „niesie pakiety transmitowane” Generalny Inspektor uznał za niefortunne i zaproponował jego przeredagowanie. Wątpliwości Generalnego Inspektora wzbudziła również definicja RAID1 (§ 2 pkt 7 projektu), którą określono jako „zabezpieczenie przed utratą danych polegające na jednoczesnym zapisie w tym samym czasie danych na dwóch pracujących w trybie kopii lustrzanej dyskach;”, podczas gdy RAID1 jest technologią polegającą na dublowaniu dysków twardych, tj. zapisywaniu tych samych danych jednocześnie na dwóch dyskach twardych. Zdaniem Generalnego Inspektora w § 2 pkt 10 projektu definicja „wersjonowania” wymaga doprecyzowania. Generalny Inspektor przedstawił również konieczność wyjaśnienia mechanizmu wersjonowania. Jak bowiem zauważył, przedstawiona w § 2 pkt 11 projektu definicja funkcji skrótu jest niejasna i nie przedstawia efektu jej wykorzystania. Natomiast w § 3 ust. 1 nie zostały określone rodzaje urządzeń rejestrujących. W projekcie tym nie został również przedstawiony zakres danych rejestrowanych w momencie popełnienia wykroczenia. Projektodawca posługuje się jedynie terminem „oraz wraz z danymi”. Zdaniem Generalnego Inspektora w § 6 ust. 3 projektu kwestia tworzenia kopii zapasowych wymaga doprecyzowania – na przykład poprzez określenie dla jakich celów są one tworzone. Natomiast w § 8 ust. 4 projektu nie określono sposobu udostępniania danych. Generalny Inspektor wskazał, iż w projekcie rozporządzenia nie określono czasu, przez jaki gromadzone są dane w urządzeniach rejestrujących. W § 8 ust. 2 pkt 3 projektu zaś postulował o uzupełnienie tej jednostki redakcyjnej o zakres żądanych obrazów i danych. Stwierdził bowiem, iż zdjęcia z urządzeń rejestrujących mogą zawierać również inne rodzaje danych czy też fragmentów obrazów, których udostępnienie z celowościowego punktu widzenia nie będzie

konieczne. Zdaniem Generalnego Inspektora, autor projektu rozporządzenia nie określił – wbrew upoważnieniu wynikającemu z delegacji ustawowej – sposobu i warunków technicznych udostępniania obrazów i danych zgromadzonych w centralnym systemie teleinformatycznym osobom lub podmiotom uprawnionym. W opinii Generalnego Inspektora wyjaśnienia wymagają również wymienione w § 10 projektu rozporządzenia „systemy teleinformatyczne, oprogramowanie i urządzenia rejestrujące użytkowane przed dniem wejścia w życie rozporządzenia” z punktu widzenia zakresu danych w nich gromadzonych, różnic lub podobieństw nowego i starego systemu, jak również celowości kopiowania danych z poprzedniego zbioru do nowego zbioru danych. Zauważyć należy, iż rozporządzenie wchodzi w życie w terminie 14 dni od dnia ogłoszenia (§ 11 projektu), natomiast do systemów teleinformatycznych, oprogramowania i urządzeń rejestrujących użytkowanych przed wejściem w życie rozporządzenia, jego przepisy stosuje się po upływie 24 miesięcy od dnia wejścia w życie (§ 10 projektu).

Generalny Inspektor wyraził swoją opinię również na temat nowej wersji wyżej opiniowanego projektu rozporządzenia, oznaczoną jako „Projekt z dnia 14.08.2012 r.”. W opinii tej Generalny Inspektor podziękował za uwzględnienie w treści przedmiotowego projektu części uwag zgłoszonych przez Generalnego Inspektora Ochrony Danych Osobowych w piśmie z dnia 26 czerwca 2012 r. oraz przedstawienie wyjaśnień w zakresie pozostałych, wyrażonych w ww. korespondencji wątpliwości. Jednocześnie podtrzymał uwagę odnoszącą się do § 6 ust. 3 projektu. Jej celem było bowiem zapewnienie precyzyjnego brzmienia tego przepisu i wskazanie jedynie przykładu dodatkowej treści, która miałyby temu służyć. Jak wyjaśnił Generalny Inspektor wątpliwość związana z brzmieniem przepisu § 6 ust. 3 projektu dotyczyła nie tyle zasadności tworzenia określonych kopii, ile braku zawarcia w nim zasad czy też procedur tworzenia kopii, które określiłyby, jak często miałyby być one wykonywane, jak również określenia danych zawartych w tzw. kopii archiwalnej, w szczególności czy kopia archiwalna miałaby zawierać dane znajdujące się w składnicy danych na określony dzień, czy też dane z konkretnego okresu czasu, podlegające usunięciu ze składnicy danych po sporządzeniu kopii archiwalnej<sup>169</sup>.

Opiniując *projekt rozporządzenia Ministra Spraw Wewnętrznych w sprawie przetwarzania informacji, w tym danych osobowych, przez Policję*<sup>170</sup>, wydawanego na podstawie delegacji zawartej w art. 20 ust. 19 ustawy z dnia 6 kwietnia 1990 roku o Policji (t. j. Dz. U. z 2011 r. Nr 287, poz. 1687 z późn. zm.), Generalny Inspektor Ochrony Danych Osobowych podkreślił, że projekt ten stanowił

---

<sup>169</sup> Prace nad projektem toczyły się również w 2013 r. Obecnie projekt posiada status obowiązującego aktu prawnego – został on ogłoszony w Dzienniku Ustaw z dnia 15 maja 2013 r. jako rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 23 kwietnia 2013 r. w sprawie obrazów i danych utrwalonych przez Głównego Inspektora Transportu Drogowego za pomocą stacjonarnych urządzeń rejestrujących zainstalowanych w pasie drogowym dróg publicznych (Dz. U. z 2013 r. poz. 565).

<sup>170</sup> DOLiS-033-547/12

pierwszą tak całościową próbę uregulowania kwestii przetwarzania przez policję informacji, w tym danych osobowych w rozumieniu art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. GODO już na wstępie wysoko ocenił przedmiotowy projekt od strony merytorycznej i wskazał, że sposób zredagowania przepisów wskazuje na dogłębne zrozumienie przez projektodawców przedmiotowej problematyki. Niemniej jednak w opinii Generalnego Inspektora nie wszystkie unormowania projektu mieszczą się w zakresie wyznaczonym przez podstawowy, wykonawczy (art. 92 ust. 1 zdanie pierwsze Konstytucji Rzeczypospolitej Polskiej) charakter aktu prawnego, jakim jest rozporządzenie. Przypomniawszy przy tym cytowane wcześniej uzasadnienie postanowienia TK z dnia 31 stycznia 2007 roku (sygn. akt S 1/2007), w którym stwierdza się, że z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie cedować funkcji prawodawczych na organy władzy wykonawczej, która nie ma kompetencji ustawodawczych ani władzy kształtowania zasadniczych elementów regulacji prawnej. Ponadto przepis art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki. Co za tym idzie, rozporządzenie nie może samodzielnie (w oderwaniu lub w swego rodzaju „uzupełnieniu” przepisów ustawy) kreować określonych zasad przetwarzania danych albo kompetencji organów. Generalny Inspektor wskazał, że z takim przypadkiem mamy do czynienia zwłaszcza w § 50–§ 52 projektu. Pierwszy z powołanych przepisów z jednej strony wskazuje sytuację, w której policja winna dokonać weryfikacji zebranych danych pod kątem ich przydatności dla realizacji jej zadań, z drugiej zaś – wprost (aczkolwiek nieenumeratywnie) wymienia podmioty, które z wnioskiem o taką weryfikację mogą do policji wystąpić. W § 51 i 52 projektu określono tymczasem przesłanki nieusuwania danych z baz danych policji (§ 51 ust. 3 część wstępna projektu), okresy przechowywania niektórych kategorii danych (§ 51 ust. 3 pkt 1 i pkt 2 projektu) oraz przesłanki usunięcia niektórych innych zebranych przez policję informacji (§ 52 ust. 4 projektu). Nie negując zatem ani potrzeby uregulowania powyższych kwestii, ani nawet redakcyjnej poprawności zaproponowanych przepisów, Generalny Inspektor Ochrony Danych Osobowych stwierdził, że nie mogą być one zamieszczone w akcie prawnym o randze rozporządzenia, gdyż narusza to zasadę hierarchiczności aktów prawnych oraz zasadę wyłączności ustawy w odniesieniu do regulacji dotyczących sfery konstytucyjnych praw i wolności obywatelskich. A do takiej zaś sfery należy prawo do prywatności (art. 47 Konstytucji Rzeczypospolitej Polskiej) oraz prawo do ochrony danych osobowych (art. 51 Konstytucji Rzeczypospolitej Polskiej) ograniczane przez przechowywanie przez policję informacji o obywatelach.

Podobny do powyższego zarzut Generalny Inspektor podniósł również w przypadku § 23 ust. 2 i § 37 ust. 6 *in fine* projektu. Oba powołane przepisy dotyczą kwestii przetwarzania danych „bez wiedzy i zgody osób, których dane te dotyczą”, przy czym pierwszy z nich statuuje uprawnienie policji

do takiego przetwarzania danych. Nie umknęło uwadze organu do spraw ochrony danych osobowych to, iż art. 25 ust. 2 pkt 1 ustawy o ochronie danych osobowych w sposób jednoznaczny stanowi, że uprawnienie do zbierania danych bez wiedzy osoby, której dane te dotyczą, musi wynikać z ustawy, a nie rozporządzenia.

Następnie Generalny Inspektor Ochrony Danych Osobowych wyraził poparcie dla konsekwentnie wyrażonej w projekcie idei, by to Komendant Główny Policji był administratorem danych przetwarzanych przez policję (§ 3 ust. 1 i 2 projektu). Wskazał też, że z niezrozumiałych dla organu do spraw ochrony danych osobowych powodów, od tej generalnie przestrzeganej zasady wprowadzony został wyjątek w § 8 ust. 1 projektu. Zgodnie bowiem z kwestionowanym przepisem likwidacja zbioru danych (łącznie z wykonanymi jego replikami) następuje na podstawie decyzji administratora zbioru (podmiotu odpowiedzialnego za administrowanie zbiorem – § 7 ust. 2 pkt 2 projektu), nie zaś administratora danych (Komendanta Głównego Policji). Skoro jednak – w myśl art. 7 pkt 4 ustawy o ochronie danych osobowych – do administratora danych należy decydowanie o celach i środkach przetwarzania danych osobowych, a Komendant Główny Policji został także bezpośrednio uprawniony do tworzenia zbiorów danych (§ 6 ust. 1 projektu), to pozbawianie go możliwości rozstrzygnięcia o likwidacji zbioru danych (i przenoszenie tej kompetencji na inny podmiot) nie wydaje się rozwiązaniem prawidłowym.

Generalny Inspektor Ochrony Danych Osobowych zwrócił również uwagę na wprowadzenie w projekcie (§ 2 pkt 16), bez wyraźnego upoważnienia ustawowego, definicji pojęcia „zbiór danych”, które to pojęcie jest już określeniem ustawowym (art. 7 pkt 1 ustawy o ochronie danych osobowych), co stanowi naruszenie § 149 *in principio* załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 roku w sprawie „Zasad techniki prawodawczej” (Dz. U. Nr 100, poz. 908). Krytycznie odniósł się również do zamieszczenia w § 22 ust. 5 projektu odesłania do „Konstytucji Interpolu”, który to dokument nie stanowi źródła prawa w rozumieniu art. 87 ust. 1 Konstytucji Rzeczypospolitej Polskiej, a zatem przepis prawa nie może do niego odsyłać<sup>171</sup>.

W odniesieniu do planowanych zmian w zakresie funkcjonowania sądownictwa w okresie sprawozdawczym 2012 roku Generalnemu Inspektorowi przedstawiono **projekt rozporządzenia Ministra Sprawiedliwości zmieniającego rozporządzenie – Regulamin urzędowania sądów powszechnych**. Początkowo zmiany związane z informatyzacją wymiaru sprawiedliwości planowano wprowadzić mocą rozporządzenia<sup>172</sup>. W trakcie prac legislacyjnych Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę, że idea informatyzacji działalności podmiotów realizujących zadania publiczne, w tym informatyzacji wymiaru sprawiedliwości, niewątpliwie zasługuje na

---

<sup>171</sup> Projekt został ogłoszony w Dzienniku Ustaw z dnia 4 kwietnia 2013 r. jako rozporządzenie Ministra Spraw Wewnętrznych z dnia 31 grudnia 2012 r. w sprawie przetwarzania informacji przez Policję (Dz. U. z 2013 r. poz. 8).

<sup>172</sup> DOLiS-033-317/12

poparcie. Jednakże uwzględniając specyfikę danych przetwarzanych na potrzeby sprawowania wymiaru sprawiedliwości przez niezależne sądy, proces ten winien być głęboko osadzony w przepisach prawa o randze ustawy. Wskazał między innymi, że przyznanie określonemu podmiotowi uprawnienia do stworzenia systemu centralnego, w którym przetwarzanych będzie szereg informacji dotyczących obywateli oraz prawa do zarządzania nimi (jego wdrażania i utrzymywania), czyli stworzenia kolejnej megabazy danych, stanowi ingerencję w sferę konstytucyjnych wolności i praw jednostek. Dane będące w tym przypadku przedmiotem przetwarzania obejmą m.in. dane szczególnie chronione, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych – a więc nie tylko dane dotyczące orzeczeń sądowych, ale również i te obejmujące dane o stanie zdrowia, wynikające z różnego rodzaju opinii psychologicznych, czy psychiatrycznych. Zatem istnienie powyższego systemu, zasady jego funkcjonowania, prawa dostępu do jego zasobów oraz ewentualne uprawnienie do cedowania kompetencji w zakresie administrowania jego zasobami na inny podmiot, powinno zostać uregulowane na szczeblu aktu ustawowego.

W związku z powyższym został przygotowany *projekt ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych*<sup>173</sup>. W uwagach do przedmiotowego projektu Generalny Inspektor wskazał, że informatyzacja sądownictwa, za którą odpowiedzialny jest Minister Sprawiedliwości, mająca polegać m.in. na projektowaniu, wdrażaniu, eksploatacji, integracji i rozwoju systemów teleinformatycznych obsługujących postępowania sądowe, czy też dostarczaniu sądom systemu teleinformatycznego służącego do udostępniania danych zawartych w aktach spraw sądowych podmiotom określonym w przepisach odrębnych (proponowany art. 175b § 2 pkt 1 i 8), może odbywać się bez wyposażenia Ministra Sprawiedliwości w prawne możliwości do „decydowania o celach i środkach przetwarzania danych osobowych” zawartych w aktach postępowań sądowych (takie bowiem uprawnienia i obowiązki wiążą się z przymiotem administratora danych). To sądy, jako sprawujące wymiar sprawiedliwości i upoważnione mocą przepisów szczególnych do przetwarzania danych osobowych – w szczególności – stron postępowania, były, są i powinny zostać administratorami tych danych. Z przepisów analizowanego projektu winno zatem wynikać, iż Minister Sprawiedliwości pozostaje wyłącznie administratorem systemu teleinformatycznego służącego do obsługi postępowania sądowego, przy czym dla tzw. czystości legislacyjnej, wartym rozważenia jest jednoznaczne wskazanie, do czego system teleinformatyczny, którego wprowadzenie się postuluje, ma służyć oraz jakie za jego pomocą można wykonywać zadania. Aktualnie dość chaotycznie proponowany art. 175b § 2 wspomina o systemie teleinformatycznym w kilku, wydaje się przypadkowo określonych, punktach.

---

<sup>173</sup> DOLiS-033-472/12

Zdaniem GIODO projektowane przepisy powinny zostać przekształcone tak, aby w pierwszej kolejności wynikało z nich, czym pozostaje używany do informatyzacji sądów system teleinformatyczny (być może wskazane byłoby posłużenie się jakąś nazwą własną, np. „Platforma.....”, „Krajowy System...”), do czego ma służyć i jakie zadania umożliwiać (np. „wykonywanie transkrypcji...”, „przechowywanie akt...”), następnie kto pozostaje jego administratorem (np. „Administratorem systemu, o którym mowa.....pozostaje Minister Sprawiedliwości”) i w związku z tym faktem, na koniec, jakie spoczywają na nim obowiązki (np. „Zadaniem administratora systemu jest techniczno–organizacyjna obsługa systemu...”). Ważnym zagadnieniem pozostaje również wskazanie, że system ten ma zapewniać, np. bezpieczeństwo przetwarzanych danych, poufność, czy pewność w procesie identyfikacji (być może należałoby zastanowić się nad potrzebą wprowadzenia odpowiedniego przepisu upoważniającego ministra do wydania stosownego aktu wykonawczego w tym zakresie). W uwagach do przedmiotowego projektu wskazano również na potrzebę wprowadzenia przepisów stanowiących o przyznawaniu prawa dostępu do systemu.

Wprowadzenie zmian w kierunku proponowanym przez organ do spraw ochrony danych osobowych miało umożliwić wykonywanie w systemie transkrypcji, czy przechowywanie akt, bez konieczności jednoczesnego wyposażania Ministra Sprawiedliwości w przymiot administratora danych przetwarzanych w związku z podejmowaniem tychże czynności.

Generalny Inspektor odniósł swoje uwagi również do proponowanego art. 175a § 1, zwłaszcza do sformułowania, iż „Minister Sprawiedliwości przetwarza dane osobowe w rejestrach prowadzonych na podstawie przepisów odrębnych”. Wskazał mianowicie, iż lapidarny i niedookreślony charakter tej regulacji również nie może zyskać akceptacji GIODO. Jeżeli celem Ministra Sprawiedliwości jest przesądzenie wprost, kiedy pozostaje on administratorem danych, których przetwarzanie przewidują inne szczególne przepisy prawa, stosownej zmiany należy dokonać w treści tychże przepisów (poprzez właściwą ich nowelizację).

Przedstawiona Generalnemu Inspektorowi Ochrony Danych Osobowych wersja projektu była wersją roboczą i do dnia sporządzenia niniejszego *Sprawozdania* projektodawca nie przedłożył nowej.

W okresie sprawozdawczym 2012 r. Generalny Inspektor poddał również analizie i ocenie pod kątem zgodności z przepisami ustawy o ochronie danych osobowych ***projekt rozporządzenia Ministra Zdrowia w sprawie określenia sposobu i organizacji leczenia krwią w podmiotach leczniczych wykonujących działalność leczniczą w rodzaju stacjonarne i całodobowe świadczenia zdrowotne***<sup>174</sup>. Podniósł w pierwszej kolejności, iż podstawowe zasady przetwarzania danych osobowych, tj. np. kwestie dotyczące ich przekazywania różnorodnym podmiotom, czy okresów przechowywania danych,

---

<sup>174</sup> DOLiS-033-292/12

w tym zwłaszcza danych szczególnie chronionych, których katalog określony został w art. 27 ust. 1 ustawy o ochronie danych osobowych, a także sprawy związane z kompetencjami do przetwarzania danych osobowych, winny każdorazowo wynikać z przepisów prawa rangi ustawy. Wskazał, że w przepisach ustawy upoważniającej, tj. ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. Nr 106, poz. 681 z późn. zm.) jest mowa jedynie o prowadzeniu przez regionalne centra krwiodawstwa i krwiolecznictwa, przez Wojskowe Centrum Krwiodawstwa i Krwiolecznictwa oraz Centrum Krwiodawstwa i Krwiolecznictwa utworzone przez ministra właściwego do spraw wewnętrznych, m.in. rejestru powikłań poprzetoczeniowych (art. 27 pkt 9). Nie jest natomiast wiadome, jakie dane w rejestrze takim się znajdują, jak długo dane tego typu są przechowywane oraz w jaki sposób poszczególne centra pozyskują informacje we wskazanym zakresie. Powstaje przy tym pytanie o zasadność posiadania przez centra krwiodawstwa wskazane w art. 4 ust. 3 pkt 2 – 4, danych o wszystkich odnotowanych nieprzewidzianych zdarzeniach (§ 13 ust. 5 projektu stanowi, iż centrum rejestruje wszystkie powikłania poprzetoczeniowe na podstawie dokumentacji przekazanej przez podmiot leczniczy). Przetwarzanie danych osobowych przez jakiegokolwiek podmioty, zwłaszcza kiedy chodzi o tzw. dane sensytywne, jako ograniczenie w prawie do ochrony danych osobowych oraz prawa do prywatności osoby, której informacje dotyczą, winno wynikać z przepisów aktu prawnego rangi ustawy.

Projektowane rozporządzenie nakładało na poszczególne podmioty obowiązek przekazywania do centrum raportów o wszelkich nieprzewidzianych zdarzeniach, a w szczególności o błędach i wypadkach, związanych z przetoczeniem (§ 5 ust. 3 pkt 6). Nie definiuje przy tym, jakiego rodzaju dane w raportach takich mają się znajdować. Także § 40 ust. 4 projektu stanowi o raportowaniu przez lekarza odpowiedzialnego za przetoczenie, błędów, które mogły zagrażać bezpieczeństwu pacjenta, do centrum bez wskazania zakresu raportowania. Pojawia się także pytanie, do którego centrum i czy do każdego, o którym stanowi art. 4 ust. 3 pkt 2 – 4 ustawy upoważniającej bliżej nieokreślone w swym zakresie raporty są przesyłane. Powyższe wątpliwe pozostawało tym bardziej, iż np. w § 7 ust. 6 projektu była mowa o przekazywaniu raportów i sprawozdań (również bez wskazania czy, a jeżeli tak to w jakim zakresie, będą w oparciu o ten przepis przesyłane dane osobowe) do właściwego centrum, choć bez wyjaśnienia, co należy pod tym pojęciem rozumieć, tj. jakie jest centrum uznawane za „właściwe”. Generalny Inspektor podniósł zatem, że brak dookreślenia ww. zakresu pozostaje w sprzeczności z tzw. zasadą adekwatności danych w stosunku do celów ich przetwarzania, statuowaną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, jak i art. 6 ust. 1 lit. c dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.WE.23.11.1995), która nakłada na administratora danych obowiązek przetwarzania (przekazywania) wyłącznie takiego zakresu danych osobowych, jaki jest niezbędny do osiągnięcia celu

tegoż przetwarzania. Aby uniknąć rozszerzającej interpretacji kwestionowanego zapisu, Generalny Inspektor zasugerował doprecyzowanie tego przepisu o zakres tych informacji, wskazując przy tym, że za tego typu doprecyzowaniem przemawiać także może treść § 25 ust. 1 w zw. z § 132 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz. U. Nr 100, poz. 908), którą trzeba mieć na uwadze formułując przepisy aktów wykonawczych. Wynika z niej, że przepis prawa materialnego powinien możliwie bezpośrednio i wyraźnie wskazywać kto, w jakich okolicznościach i jak powinien się zachować (przepis prawa materialnego).

Wątpliwości Generalnego Inspektora wzbudzało także takie ukształtowanie przepisów projektu, że wynikało z nich, iż dokumentację dotyczącą leczenia krwią i jej składnikami umożliwiającą prześledzenie losów przetoczenia i związanych z tym badań, przechowuje się co najmniej przez 30 lat od dnia jej sporządzenia. Istotną z punktu widzenia przepisów ustawy o ochronie danych osobowych jest bowiem tzw. zasada ograniczenia czasowego, wynikająca z art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych. W sytuacji, kiedy z brzmienia przepisu nie wynika „sztywna” data przechowywania dokumentacji, dochodzić może do przetwarzania danych osobowych w niej zawartych zbyt długo, wręcz w nieskończoność, czyli w sprzeczności z zasadami wynikającymi z przepisów o ochronie danych osobowych (§ 6 ust. 1 projektu).

W kolejnej korespondencji dotyczącej tego projektu, Generalny Inspektor Ochrony Danych Osobowych wyraził pełną aprobatę z powodu uwzględnienia wcześniej sygnalizowanych przez niego uwag, w tym w szczególności za zapewnienie o przeniesieniu na grunt ustawowy wszelkich, istotnych z punktu widzenia zasad przetwarzania danych osobowych, o których stanowi ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, kwestii objętych materią projektowanego rozporządzenia<sup>175</sup>.

Na szczególną uwagę zasługują opiniowane w 2012 roku przez Generalnego Inspektora Ochrony Danych Osobowych *projekty rozporządzeń Ministra Zdrowia dotyczące systemu Elektronicznej Weryfikacji Uprawnnień Świadczeniobiorców, zwanego e-WUŚ*<sup>176</sup>. W pierwszym z opiniowanych projektów – tj. w *projekcie rozporządzenia Ministra Zdrowia w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej* - wątpliwości pod kątem zgodności z przepisami ustawy o ochronie danych osobowych budziło przede wszystkim wprowadzanie przepisami przedłożonego projektu „systemu Elektronicznej Weryfikacji

---

<sup>175</sup> Projekt został ogłoszony w Dzienniku Ustaw z dnia 4 stycznia 2013 r. jako projekt rozporządzenia Ministra Zdrowia z dnia 11 grudnia 2012 r. w sprawie leczenia krwią w podmiotach leczniczych wykonujących działalność leczniczą w rodzaju stacjonarne i całodobowe świadczenia zdrowotne, w których przebywają pacjenci ze wskazaniami do leczenia krwią i jej składnikami (Dz. U. z 2013 r. poz. 5).

<sup>176</sup> DOLiS-033-544/12 - projekt rozporządzenia Ministra Zdrowia w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej oraz projekt rozporządzenia Ministra Zdrowia w sprawie sposobu, trybu i terminów występowania do Narodowego Funduszu Zdrowia oraz udostępniania przez Narodowy Fundusz Zdrowia świadczeniobiorcom informacji o prawie do świadczeń opieki zdrowotnej oraz udzielonych mu świadczeniach.



Uprawnień Świadczeniobiorców” (e-WUŚ). Generalny Inspektor zwrócił uwagę, że sam fakt istnienia takiego systemu winien być bowiem przewidziany przepisami o randze ustawy. Powyższe zyskuje na znaczeniu, gdyby wziąć pod uwagę, że tytuł rozporządzenia, związany z brzmieniem delegacji ustawowej (art. 50 ust. 4 ustawy z dnia 27 lipca 2012 r. o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych – Dz. U. z 2012 r. poz. 1016) odnosi się do „warunków występowania o sporządzanie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej”. Generalny Inspektor Ochrony Danych podkreślił, że tym samym wprowadzanie w projekcie przepisów stanowiących o funkcjonowaniu systemu Elektronicznej Weryfikacji Uprawnień Świadczeniobiorców może wykraczać poza ramy przepisów upoważniających.

Ponadto projekt rozporządzenia, w opinii Generalnego Inspektora, określał zbyt lapidarnie „warunki, jakie muszą spełniać świadczeniodawca lub niebędąca świadczeniodawcą osoba uprawniona w rozumieniu art. 2 pkt 14 ustawy o refundacji, występujący do funduszu o dokument elektroniczny, o którym mowa w ust. 3”. Generalny Inspektor zwrócił uwagę, na przykład, na brak informacji w zakresie wymogów dla systemu teleinformatycznego, za pomocą którego dochodzić będzie do sporządzania dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej. Nie jest przy tym wystarczające zawarcie w treści projektów przepisów nakładających na świadczeniodawcę lub niebędącą świadczeniodawcą osobę uprawnioną, zobowiązanie do „przestrzegania przepisów o ochronie danych osobowych” (§ 3 ust. 2 pkt 2a projektu), albowiem wobec takiej czy innej budowy właściwych systemów, tego typu deklaracje mogą pozostać bez znaczenia. Innymi słowy, błędy w konstruowaniu odpowiednich systemów mogą mieć bezpośredni wpływ na kwestie bezpieczeństwa przetwarzanych w nich danych osobowych i możliwości stosowania odpowiednich środków bezpieczeństwa przez same osoby zainteresowane.

Generalny Inspektor wskazał również na wątpliwości, jakie budziło sformułowanie „uprawnienie do potwierdzania prawa do świadczeń opieki zdrowotnej” pod kątem jego poprawności i tego, czy oddaje istotę zagadnienia (§ 2 projektu). Celem wdrożenia przedmiotowej regulacji – jak wynika z treści uzasadnienia do projektu rozporządzenia – było bowiem zapewnienie świadczeniodawcom możliwości weryfikowania statusu ubezpieczenia, nie zaś potwierdzanie prawa do przysługujących danej osobie świadczeń opieki zdrowotnej. Biorąc powyższe pod uwagę zasadnym wydaje się stosowne przereformowanie przedmiotowego zwrotu. Generalny Inspektor wskazał również, że przekazywanie danych osobowych osobom trzecim, nieuprawnionym do ich pozyskiwania, rodzi odpowiedzialność karną, o której jest mowa w przepisach ustawy o ochronie danych osobowych. Zastanowienia wymaga więc, w jakich kategoriach należy traktować rygor utraty upoważnienia do korzystania z systemu eWUŚ, przewidywany w treści § 3 ust. 2 pkt 2b projektu, niezależnie od podniesionej we wstępie wątpliwości w kwestii prawnej możliwości wprowadzania samego systemu w oparciu o przepisy aktu wykonawczego. Ponadto w opinii Generalnego Inspektora wartym

rozważenia było również wskazanie, w jakiej postaci (elektronicznej, czy też papierowej) ma być składany wniosek o uzyskanie upoważnienia, czego w przepisach nie uregulowano. Spośród innych uwag skierowanych do tego projektu Generalny Inspektor podniósł, że pojęcie „lokalny administrator systemu Elektronicznej Weryfikacji Upoważnień Świadczeniobiorców” powinno zostać uwzględnione w przepisach samej ustawy upoważniającej, gdzie określone powinny zostać również uprawnienia i obowiązki związane z pełnieniem takiej roli, jak również, że w opiniowanych przepisach brak jest wyjaśnienia czym ma być „Portal dostępowy Funduszu”. Abstrahując od niepoprawnie użytego sformułowania „portal”, w rozporządzeniu nie znajdziemy informacji, o jaki serwis internetowy chodzi, czy jest on witryną informacyjną, czy Biuletynem Informacji Publicznej, czy jest regulowany przez prawo, a jeśli nie, to jakie zabezpieczenia związane z koniecznością przesyłania za jego pomocą danych osobowych są w nim stosowane. GODO zakłada, że ów serwis internetowy będzie podlegał wymaganiom ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i aktów wykonawczych do tej ustawy, lecz uznaje jednocześnie, że sformułowanie „Portal dostępowy Funduszu” nie jest pojęciem prawnym, a przywoływane jest tak jakby nim było.

Podsumowując Generalny Inspektor wskazał, iż analizowany projekt powinien w pierwszej kolejności odpowiadać na pytanie, kto, w jakich sytuacjach, kiedy, i po spełnieniu jakich warunków technicznych i organizacyjnych (tak ze strony świadczeniodawcy jak i niebędącej świadczeniodawcą osoby fizycznej) może podejmować działania w zakresie sporządzania dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej oraz wskazywać odpowiednie zabezpieczenia, konieczność stosowania których pociąga za sobą przetwarzanie danych osobowych, zwłaszcza poprzez sieci teleinformatyczne. Zasugerował przy tym, że w tym celu do przepisów projektu należałoby przenieść niektóre – prawidłowe skądinąd – rozwiązania zawarte w opracowanym niegdyś „Regulaminie korzystania przez świadczeniodawców z systemu Elektronicznej Weryfikacji Upoważnień Świadczeniobiorców”, które w sposób szczegółowy odnoszą się do przedmiotowego zagadnienia.

Spośród uwag dotyczących projektu ***rozporządzenia Ministra Zdrowia w sprawie sposobu, trybu i terminów występowania do Narodowego Funduszu Zdrowia oraz udostępniania przez Narodowy Fundusz Zdrowia świadczeniobiorcom informacji o prawie do świadczeń opieki zdrowotnej oraz udzielonych mu świadczeniach***, należy wskazać na wyrażoną przez Generalnego Inspektora wątpliwość, czy wystarczającą gwarancją bezpieczeństwa przetwarzanych danych osobowych – w zakresie konieczności udostępniania informacji wyłącznie osobom uprawnionym – będzie wskazanie przez projektodawcę na możliwość udostępnienia przez Narodowy Fundusz Zdrowia informacji, w sytuacji wskazania przez wnioskodawcę w treści wniosku błędnego adresu zamieszkania oraz (jak wynika z treści § 4 ust. 2 pkt 2 w zw. § 3 ust. 3 lit. b projektu) adresu do korespondencji. W opinii

GIODO, rozwiązaniem właściwym z punktu widzenia bezpieczeństwa przetwarzanych danych byłoby żądanie zamieszczania we wniosku adresu zameldowania, oraz zwracanie wniosku także w sytuacji podania przez wnioskodawcę mylnego adresu zameldowania.

Generalny Inspektor zgłosił również uwagi dotyczące przesyłania wniosków o udostępnianie informacji m.in. pocztą elektroniczną. Z § 3 ust. 2 projektu wynikało, że wniosek o udostępnienie informacji, o którym mowa w ust. 1 tego przepisu, przesyła się m.in. pocztą elektroniczną. Wniosek składany w postaci elektronicznej musi być podpisany „bezpiecznym podpisem” albo podpisem potwierdzonym profilem zaufanym w e-PUAP (ust. 6 w pkt. 2). Generalny Inspektor zwrócił również uwagę, że możliwość używania poczty elektronicznej do przesyłania korespondencji do NFZ stwarza ryzyko naruszenia poufności danych zawartych we wniosku. Wobec powyższego należałoby zastanowić się nad wprowadzeniem możliwości wysyłania wniosków za pomocą środków komunikacji elektronicznej przy zachowaniu wymagań wskazanych w rozporządzeniu Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. Nr 206, poz. 1216). Środkami takimi mogą być np. skrzynka podawcza instytucji, do której wnioski mają być składane, platforma ePUAP lub inne rozwiązania, których stosowanie uczyni zadość wymogom wynikającym z przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565 z późn. zm.). Ponadto w opinii Generalnego Inspektora Ochrony Danych Osobowych wszystkie proponowane przepisami projektu rozwiązania, które ograniczają możliwość udostępniania lub otrzymywania przez Fundusz informacji drogą elektroniczną (np. § 5, czy § 6 ust. 1), wymagają jednocześnie analizy pod kątem zgodności z art. 14 ust. 3 ww. ustawy. Z treści powołanego przepisu wynika bowiem, iż podmiot publiczny prowadzący rejestr publiczny jest obowiązany umożliwić dostarczanie informacji do tego rejestru oraz udostępnianie informacji z tego rejestru drogą elektroniczną w przypadku, gdy ten rejestr działa przy użyciu systemów teleinformatycznych.

Generalny Inspektor wskazał również, że wprowadzając rozwiązanie przyznające prawo do korzystania z informacji zawartych w „systemie informatycznym” (§ 6 ust. 1 projektu) Funduszu w sposób bezpośredni, tzn. poprzez przyznawanie prawa korzystania z systemu informatycznego osobie zainteresowanej uzyskaniem informacji, pominięto zupełnie kwestie wymogów dla ww. systemu, których spełnienie mogłoby się przyczynić do zapewnienia skutecznej ochrony danych osobowych przed nieuprawnionym dostępem czy ujawnieniem (np. czy odpowiednie łącze będzie zabezpieczone kryptograficznie, czy system będzie odnotowywał informację w zakresie logowania się do systemu przez poszczególne osoby uprawnione, oraz czy te osoby będą miały wyłącznie prawo do przeglądania informacji, czy też także prawo do ich edytowania). Powyższe miało tym donioślejsze znaczenie, że ryzyko związane z nieuprawnionym dostępem do danych gwałtownie rośnie w obliczu

umożliwiania dużej liczbie osób korzystanie z informacji zawartych w określonych systemach informatycznych administratora danych (w tym przypadku Funduszu).

Kolejną istotną uwagę kierowaną do tego projektu było zastrzeżenie dotyczące dopuszczalności rozwiązania przewidzianego w § 6 ust. 2 pkt 2 projektu, zgodnie z którym jednym z warunków uzyskania przez świadczeniobiorcę prawa do korzystania z systemu informatycznego Funduszu jest podpisanie pomiędzy tym świadczeniobiorcą a Funduszem, umów upoważniających do korzystania z systemu. Generalny Inspektor zwrócił uwagę, że zasadnicze kwestie określające prawa i obowiązki z jednej strony administratora danych, z drugiej zaś osoby, której dane te dotyczą, winny być przedmiotem regulacji powszechnie obowiązujących przepisów prawa, nie zaś bliżej nieokreślonych umów, tym bardziej w sytuacji, kiedy trudno mówić o równości podmiotów w zakresie dowolnego kształtowania ich treści. Dlatego też wszelkie wymogi, których spełnienie warunkuje możliwość korzystania z systemu przez świadczeniobiorcę, powinny zostać wskazane w treści opiniowanego projektu.

Ponadto organ do spraw ochrony danych osobowych podniósł, że względy bezpieczeństwa oraz wymagania wskazane w rozporządzeniu 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) sprzeciwiają się proponowanej treści § 8 ust. 5 projektu, zgodnie z którą „Dane dostępne są ważne bezterminowo.” W opinii Generalnego Inspektora nie można bowiem dopuścić do sytuacji prawnej, zgodnie z którą szczególne wobec przepisów o ochronie danych osobowych akty prawne przewidują rozwiązania mniej restrykcyjne w kwestii obowiązków administratora danych w zakresie bezpieczeństwa ich przetwarzania, aniżeli sama ustawa i wydane na jej podstawie akty wykonawcze. Załącznik do ww. rozporządzenia w części A.IV w pkt. 2 wyraźnie stanowi, że, cyt.: „(...) w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków (...)”. Wprowadzenie rozwiązania innego, niż to określone w rozporządzeniu MSWiA, mogłoby nastąpić tylko wówczas, gdyby wskazane zostały inne rozwiązania techniczne lub organizacyjne, które umożliwiłyby nadawanie świadczeniobiorcy hasła bezterminowo.

GIODO wskazał również, że w treści § 7 ust. 4 projektu brak jest jakichkolwiek wskazówek w zakresie rodzaju środków zapewniających poufność przekazania, jakie należy zastosować w przypadku wydawania tzw. „danych dostępowych”. Mamy tu określenie o treści „Dane dostępne wydaje się z zachowaniem środków zapewniających poufność przekazania”, które jest tu niewystarczające oraz prowadzić może do powstania wątpliwości interpretacyjnych.

W nawiązaniu do pisma z dnia 8 grudnia 2012 r. dotyczącego prac nad **projektem rozporządzenia Ministra Zdrowia w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej**, Generalny Inspektor z jednej strony dziękując za uwzględnienie niektórych uwag sygnalizowanych wcześniej wskazał, że wciąż aktualne pozostaje stanowisko GIODO w zakresie pozostałych. Generalny Inspektor stwierdził m.in., że projekt winien stanowić wprost o warunkach, jakie muszą być spełnione w przypadku występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej. Uwzględniając brzmienie delegacji ustawowej z art. 50 ust. 4 ustawy z dnia 27 lipca 2012 r. o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2012 r. poz. 1016), z treści której wynika, iż minister właściwy do spraw zdrowia określi w drodze rozporządzenia warunki, jakie muszą spełniać świadczeniodawca lub niebędąca świadczeniodawcą osoba uprawniona występująca do Funduszu o dokument elektroniczny, na podstawie którego ma być potwierdzone jej prawo do świadczeń opieki zdrowotnej, nie sposób było uznać, iż wydane na takiej podstawie rozporządzenie może pomijać wszystkie te kwestie natury organizacyjno–technicznej, których spełnienie warunkuje uznanie procesu przetwarzania danych osobowych za dostatecznie bezpieczny i wypełnienie tym samym wytycznych zawartych w delegacji ustawowej („mając na uwadze zapewnienie integralności oraz poufności przetwarzanych danych”).

Konieczność projektowania aktów prawnych w sposób czytelny i zrozumiały dla podmiotów stosujących przyjmowane rozwiązania, w praktyce nakazuje całościowe wskazanie w ich przepisach rozwiązań, jakie – celem osiągnięcia zamierzonego efektu – należy wdrażać. Generalny Inspektor zwrócił uwagę, że projekt rozporządzenia w sposób wyłącznie pobieżny odnosi się do istoty tego zagadnienia. W zupełności pomija kwestie stosowanych zabezpieczeń w zakresie choćby sposobów uwierzytelniania użytkowników w systemie informatycznym, czy weryfikowania składanych na jego podstawie wniosków. Nie odnosi się on w żaden sposób do wymogów dla systemu teleinformatycznego, który ma być skądinąd stosowany do przetwarzania danych osobowych.

Zdaniem Generalnego Inspektora, kompleksowa regulacja nowatorskich przedsięwzięć, jakie przewiduje projekt, winna polegać na wskazaniu w przepisach procedowanego rozporządzenia w sposób wyraźny, kto i w jakim celu ma mieć dostęp do systemu informatycznego o nazwie „usługa Elektronicznej Weryfikacji Upnień Świadczeniobiorców” oraz po spełnieniu jakich warunków (zwłaszcza uwzględniając elektroniczny charakter usługi, w zakresie wymogów dla nadawania loginów, haseł dostępowych, kluczy dostępu). Należy pamiętać, iż rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zawiera jedynie pewne niezbędne minimum w zakresie zabezpieczeń systemów

teleinformatycznych i w interesie administratorów danych jest stosowanie rozwiązań zapewniających dalej idącą ochronę przetwarzanym za jego pośrednictwem danych osobowych, co mogłoby w praktyce pomóc w zapobieganiu nadużyciom i skutecznie eliminować ryzyko udostępniania danych osobom nieupoważnionym<sup>177</sup>.

Kolejna, warta przedstawienia w niniejszym *Sprawozdaniu*, opinia GIODO dotyczyła **projektu rozporządzenia Ministra Zdrowia w sprawie utworzenia Krajowego Rejestru Nowotworów**<sup>178</sup>. Generalny Inspektor wskazał, że przedłożony projekt nie stanowi prawidłowego wykonania upoważnienia ustawowego zawartego w art. 19 ust. 1 i art. 20 ust. 1 ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 z późn. zm.), gdyż – wbrew jednoznaczemu brzmieniu art. 20 ust. 1 pkt 5 tejże ustawy – nie precyzuje zakresu danych przetwarzanych w Krajowym Rejestrze Nowotworów. Za takim stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych jednoznacznie przemawia brzmienie § 7 analizowanego projektu rozporządzenia Ministra Zdrowia, który to przepis zamiast – jak precyzyjnie stanowi art. 20 ust. 1 pkt 5 ustawy o systemie informacji w ochronie zdrowia – określać: „zakres i rodzaj danych przetwarzanych w rejestrze spośród danych określonych w art. 4 ust. 3 i art. 19 ust. 6” (ustawy o systemie informacji w ochronie zdrowia), odsyła do bliżej niezdefiniowanych unormowań zawartych w przepisach wydanych na podstawie art. 31 ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej (t. j. Dz. U. z 2012, poz. 591). Taka konstrukcja projektu nie mogła zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych i to z trzech zasadniczych powodów. Po pierwsze - rozwiązanie przyjęte w obowiązującej ustawie o systemie informacji w ochronie zdrowia (art. 20 ust. 1 zdanie pierwsze) polegające na dopuszczeniu, by rejestry medyczne (w tym Krajowy Rejestr Nowotworów) były konstruowane w oparciu o akty prawne niższego rzędu, aniżeli ustawy (rozporządzenia Ministra Zdrowia), stanowi wyjątek od – statuowanego w art. 27 ust. 2 pkt 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – wymagania, by przetwarzanie danych szczególnie chronionych (a do takiej kategorii należą zawarte w rejestrach medycznych dane o stanie zdrowia – art. 27 ust. 1 ustawy o ochronie danych osobowych) odbywało się w oparciu o przepisy szczególne rangi ustawowej. Wyjątek taki – zgodnie z zasadą *exceptiones non sunt extendendae* – nie może być interpretowany rozszerzająco i niejako legalizować przetwarzania danych szczególnie chronionych na podstawie przepisów rozporządzeń wydanych w oparciu o inne ustawy, niż ustawa o systemie informacji w ochronie zdrowia. Do takiej zaś swoistej legalizacji przepisów wykonawczych do ustawy o statystyce

---

<sup>177</sup> Projekty niniejszych rozporządzeń zyskały status obowiązujących aktów prawnych –rozporządzenie Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej (Dz. U. z 2012 r. poz. 1500), rozporządzenie Ministra zdrowia w sprawie sposobu, trybu i terminów występowania do Narodowego Funduszu Zdrowia oraz udostępniania przez Narodowy Fundusz Zdrowia świadczeniobiorcom informacji o prawie do świadczeń opieki zdrowotnej oraz udzielonych mu świadczeniach (Dz. U. z 2012 r. poz. 1505).

<sup>178</sup> DOLiS-033-516/12

publicznej (w tym rozporządzenia wydawanego na podstawie delegacji zawartej w art. 31 tejże ustawy), prowadziłyby zaproponowana w projekcie dyspozycja § 7. Po drugie, organ do spraw ochrony danych osobowych już od kilku lat wskazuje na wadliwość ustawy o statystyce publicznej i prowadzi w tej kwestii obszerną korespondencję z Głównym Urzędem Statystycznym, jak również m.in. z Ministerstwem Zdrowia. W korespondencji tej podnosi, że obowiązująca ustawa o statystyce publicznej (wbrew wymogom konstytucyjnym oraz wynikającym z przepisów o ochronie danych osobowych) przekazuje do unormowania w przepisach podstawowych (wykonawczych) zagadnienia o zasadniczym znaczeniu, w tym dotyczące problematyki przetwarzania danych szczególnie chronionych. W ostatnim czasie wyrażany przez Generalnego Inspektora Ochrony Danych Osobowych pogląd co do nieprawidłowości ustawy o statystyce publicznej, zyskał poparcie ze strony Rady Legislacyjnej przy Prezesie Rady Ministrów. W tym stanie rzeczy budzić musiało zdziwienie organu do spraw ochrony danych osobowych sytuacja, w której autor projektu, znając negatywne stanowisko Generalnego Inspektora Ochrony Danych Osobowych wobec dyspozycji art. 31 ustawy o statystyce publicznej, zdecydował się jednak na zastosowanie w § 7 projektu odesłania do tego przepisu. Istnienie takiego odesłania (jak wykazano to już wyżej) sugerowałoby, iż art. 31 ustawy o statystyce publicznej (przekazujący do uregulowania w rozporządzeniu Prezesa Rady Ministrów całość zagadnienia przetwarzania danych przez służby statystyki publicznej, w tym przetwarzania danych szczególnie chronionych) jest jednak przepisem prawidłowym, z czym Generalny Inspektor Ochrony Danych Osobowych zdecydowanie nie mógł się zgodzić. Po trzecie, organ do spraw ochrony danych osobowych zwrócił uwagę, że skoro ustawodawca zdecydował się powierzyć (art. 20 ust. 1 pkt 5 ustawy o systemie informacji w ochronie zdrowia) Ministrowi Zdrowia określenie zakresu i rodzaju danych przetwarzanych w Krajowym Rejestrze Nowotworów, to minister ten nie może cedować tego obowiązku na inny podmiot. Do takiej zaś sytuacji doszłoby w przypadku przyjęcia projektu w zaproponowanym kształcie. Zgodnie bowiem z dyspozycją powoływanego w § 7 projektu, art. 31 ustawy o statystyce publicznej, rozporządzenie wykonawcze kreujące kartę zgłoszenia nowotworu złośliwego wydaje Prezes Rady Ministrów, nie zaś Minister Zdrowia. Tym samym to Prezes Rady Ministrów decydowałby (wbrew dyspozycji art. 20 ust. 1 pkt 5 ustawy o systemie informacji w ochronie zdrowia) o zakresie danych przetwarzanych w Krajowym Rejestrze Nowotworów. Na zakończenie GODO wskazał, że w przedstawionej formie przedmiotowy projekt nie może być zaakceptowany przez organ do spraw ochrony danych osobowych. Dopiero po zmianie brzmienia projektu w takim stopniu, by projekt ten spełniał wymagania zawarte w art. 19 ust. 1 i art. 20 ust. 1 ustawy o systemie informacji w ochronie zdrowia, tzn. by precyzyjnie określał zakres danych podlegających przetwarzaniu w Krajowym Rejestrze Nowotworów, będzie on władny wyrazić szczegółowe stanowisko w przedmiocie zgodności tego projektu z przepisami ustawy o ochronie danych osobowych. Zauważył również, że błędne jest brzmienie § 3 ust. 2 pkt 2 projektu, zgodnie

z którym jednym z celów Krajowego Rejestru Nowotworów jest: „zasilanie danymi systemu informacji w ochronie zdrowia...”. Zgodnie bowiem z art. 5 ust. 1 pkt 3 ustawy o systemie informacji w ochronie zdrowia, Krajowy Rejestr Nowotworów, jako jeden z rejestrów medycznych, będzie stanowić element systemu informacji w ochronie zdrowia, a zatem nie może być mowy o jakimkolwiek przekazywaniu danych z Krajowego Rejestru Nowotworów do systemu informacji w ochronie zdrowia, co sugeruje aktualne brzmienie § 3 ust. 2 pkt 2 projektu<sup>179</sup>.

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

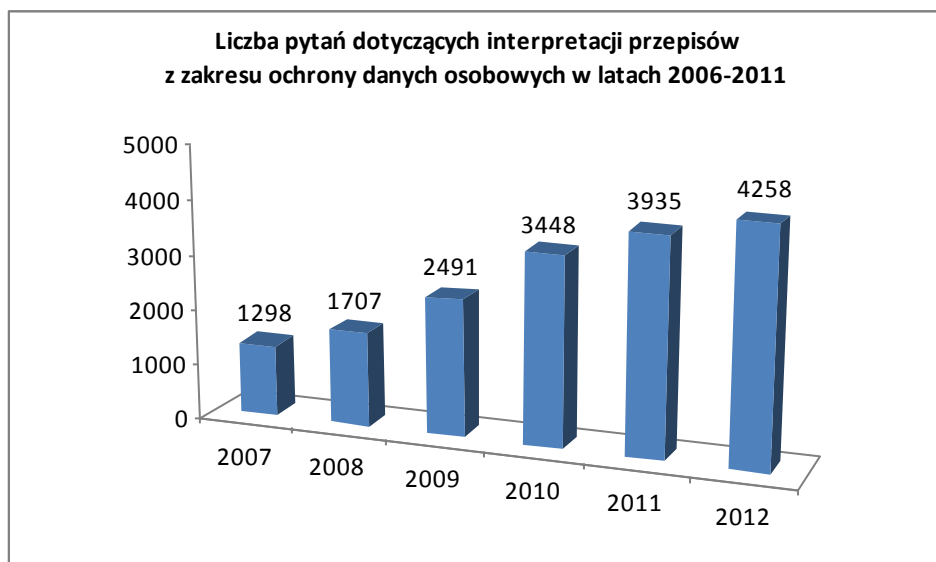
Udzielanie odpowiedzi na pytania dotyczące legalności przetwarzania danych osobowych stanowi istotny element działalności informacyjnej i edukacyjnej Generalnego Inspektora Ochrony Danych Osobowych. Należy przy tym wskazać, że problematyka ta pozostaje przedmiotem zainteresowania szerokiej i zarazem zróżnicowanej grupy interesantów i że zainteresowanie to systematycznie wzrasta.

W analizowanym okresie 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **4258 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 2011 wpłynęło 3935 pytań prawnych z zakresu ochrony danych osobowych, zaś w 2010 r. – 3448, 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 2007–2012 przedstawia *Wykres 40*.

---

<sup>179</sup> Projekt tego rozporządzenia z dnia 20 grudnia 2012 r. opublikowany został w Dzienniku Ustaw z 2012 r. poz. 1497.





*Wykres 40: Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GODO w latach 2007–2012.*

W porównaniu z ubiegłym rokiem, w okresie objętym niniejszym *Sprawozdaniem*, o 323 zwiększyła się liczba pytań, które wpłynęły do organu do spraw ochrony danych osobowych. Nadawcami największej liczby pytań były osoby fizyczne, w tym osoby prowadzące działalność gospodarczą.

Spośród 4258 pism zawierających pytania z zakresu ochrony danych osobowych, 11 % stanowiły pytania związane z rejestracją zbiorów, 9 % - udostępniania danych, 7,3 % - dotyczyło kwestii zgody na przetwarzanie danych, 4,7 % - postępowania z dokumentami zawierającymi dane osobowe, 7,2 % - wprost dotyczyło Internetu, zaś 3 % odnosiło się do zagadnień związanych z usuwaniem danych osobowych.

## **7.1. Interpretacja przepisów**

Przedstawiona poniżej analiza **pytań prawnych**, które w 2012 r. wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych, w głównej mierze dotyczyć będzie działalności różnych instytucji publicznych, banków, zakładów opieki zdrowotnej, wspólnot oraz spółdzielni mieszkaniowych, podmiotów świadczących usługi w sieci, a także zagadnień związanych z rejestracją zbiorów danych osobowych, działalnością marketingową i windykacją.

### 7.1.1. Podmioty świadczące usługi z zakresu ochrony zdrowia

W roku 2012 Generalny Inspektor Ochrony Danych Osobowych analizował szereg istotnych zagadnień dotyczących przetwarzania danych w działalności podmiotów świadczących usługi z zakresu ochrony zdrowia.

Jedno z interesujących pytań przesłanych zostało do Biura GODO od Podsekretarza Stanu z Ministerstwa Zdrowia. Dotyczyło ono **wniosku w sprawie udostępnienia danych osób pozbawionych wolności, którym zespoły ratownictwa medycznego udzielały świadczeń zdrowotnych**. W odpowiedzi<sup>180</sup> Generalny Inspektor zaznaczył, że przedstawione w treści korespondencji okoliczności sprawy ujęte zostały w sposób zbyt lakoniczny, aby na ich podstawie można było ocenić zasadność żądania przez Dyrektora Generalnego Służby Więziennej informacji wskazanych w treści pytania. Generalny Inspektor przypomniał, iż ustawa o ochronie danych osobowych nakłada na administratora danych szereg obowiązków. Wśród nich znajduje się m.in. obowiązek legitymowania się jedną z przesłanek legalności przetwarzania danych osobowych, które określone zostały w art. 23 ust. 1 pkt 1 – 5 – w stosunku do przetwarzania danych tzw. zwykłych (jak np. imię, nazwisko, adres zamieszkania) oraz w art. 27 ust. 2 pkt 1 – 10, gdy przetwarzanie dotyczy danych szczególnie chronionych, wymienionych w art. 27 ust. 1, i do których zalicza m.in. dane o stanie zdrowia. Generalny Inspektor podkreślił, iż podmioty z sektora publicznego, które – zgodnie z art. 7 Konstytucji Rzeczypospolitej Polskiej – wiąże zasada legalizmu – muszą opierać swoje działanie na przesłance określonej w art. 23 ust. 1 pkt 2 lub art. 27 ust. 2 pkt 2 przywoływanej ustawy. Dla wykonywania jakichkolwiek operacji na danych osobowych natury szczególnie chronionej (bo do tego rodzaju danych należy zaliczyć informację o konkretnej osobie, w zakresie dotyczącym m.in. nazwy i numeru statystycznego Międzynarodowej Klasyfikacji Chorób i Problemów Zdrowotnych przypisanych tej osobie), czyli także dla ich udostępnienia, wymagane jest istnienie przepisu rangi ustawy stwarzającego pełne gwarancje ochrony danych. Generalny Inspektor zaznaczył, iż w zasygnalizowanym przypadku to przepisy tzw. „ustaw sektorowych”, w tym m.in. ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. Nr 191, poz. 1410 z późn. zm.) oraz ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. Nr 112, poz. 654 z późn. zm.) winny stanowić punkt wyjścia do rozważań na temat istnienia lub braku podstawy prawnej do udostępnienia wnioskowanych danych. Z punktu widzenia ustawy o ochronie danych osobowych, istotną pozostaje zasada adekwatności danych w stosunku do celów ich przetwarzania. Generalny Inspektor podniósł także, że jeżeli administrator uzurpuje sobie więcej praw, niż przewidują obowiązujące przepisy prawa, następuje zachwianie omówionej równowagi na korzyść administratora, a zatem ma miejsce bezpodstawne ograniczenie praw osoby, której dane dotyczą. W procesie

---

<sup>180</sup> DOLiS-035-1708/12/40677

przetwarzania danych osobowych (czy to pozyskując, czy też udostępniając dane osobowe) należy mieć na uwadze proporcjonalność przetwarzanych danych w stosunku do rzeczywistej potrzeby ich posiadania przez podmioty w procesie tym uczestniczące. Abstrahując od nieprecyzyjnie opisanego stanu faktycznego należało zastanowić się, czy dla dokonania analizy zjawiska niezbędne było dysponowanie danymi osobowymi więźnia (imię, nazwisko, nr PESEL). Generalny Inspektor Ochrony Danych Osobowych zadał pytanie, czy celu, w jakim dane miały być przekazane, nie można było osiągnąć przy użyciu informacji o charakterze „bardziej statystycznym”, niż podawanie danych identyfikujących podmiot.

Generalny Inspektor odpowiadał również na pytanie<sup>181</sup>, **czy szpital miał prawo przekazać Rzecznikowi Praw Pacjenta księgi odmów przyjęć i porad ambulatoryjnych wykonywanych w izbie przyjęć szpitala.** W odpowiedzi Generalny Inspektor wskazał, że kwestie udostępnienia Rzecznikowi Praw Pacjenta określonych danych osobowych w związku z wykonywaniem przez niego ustawowych zadań, powinna być rozpatrywana w oparciu o przepisy ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t. j. Dz. U. z 2012 r. poz. 159). Mając na uwadze normy rozdziału 12 cytowanej ustawy, regulujące funkcjonowanie centralnego organu administracji rządowej właściwego w sprawach ochrony praw pacjentów określonych w niniejszej ustawie oraz w przepisach odrębnych, jakim jest Rzecznik Praw Pacjenta, Generalny Inspektor zauważył, że podmiot ten podejmuje działania w granicach kompetencji określonych stosownymi, powszechnie obowiązującymi przepisami. Jak stanowi art. 47 ust. 1 pkt 1 ww. aktu prawnego, do zakresu działania Rzecznika należy m.in. prowadzenie postępowań w sprawach praktyk naruszających zbiorowe prawa pacjentów. W celu wszechstronnego zbadania danej sprawy, Rzecznik Praw Pacjenta musi uzyskiwać dostęp do określonych dokumentów, w tym do dokumentacji medycznej, co wynika z szczególności z treści art. 61 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Zgodnie z tym przepisem, Rzecznik ma prawo żądać przedstawienia dokumentów oraz wszelkich informacji dotyczących okoliczności stosowania praktyk, co do których istnieje uzasadnione podejrzenie, że naruszają zbiorowe prawa pacjentów, w terminie nie dłuższym niż 30 dni od dnia otrzymania żądania. Żądanie, o którym mowa w ust. 1, powinno zawierać wskazanie zakresu informacji, celu żądania, terminu udzielania informacji oraz pouczenie o sankcjach za nieudzielanie informacji lub za udzielenie informacji nieprawdziwych lub wprowadzających w błąd (ust. 2 ww. przepisu). Zgodnie z art. 26 ust. 3 pkt 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną również 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,

---

<sup>181</sup> DOLiS-035-748/12/19597

w szczególności kontroli i nadzoru. Generalny Inspektor odniósł powyższe do zasad ochrony danych osobowych, w szczególności do przepisów art. 27 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, który reguluje sytuacje dopuszczalności przetwarzania danych szczególnie chronionych, w tym danych o stanie zdrowia. Wskazał następnie, że uprawnienie Rzecznika Praw Pacjenta do dostępu do danych sensytywnych zawartych w dokumentacji medycznej w związku z prowadzonymi z urzędu czynnościami wyjaśniającymi, wynika z przepisów szczególnych. A zatem spełniona zostaje przesłanka z art. 27 ust. 1 pkt 2 ustawy o ochronie danych osobowych, tj. przetwarzanie danych, o których mowa w ust. 1, jest dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. Przesłanki zezwalające na przetwarzanie danych tzw. szczególnie chronionych, określone w art. 27 ust. 2 pkt 1 – 10 są równoprawne. Zgoda jest jedynie jednym z warunków, po spełnieniu którego istnieje możliwość przetwarzania danych wrażliwych, a zatem w sytuacji, gdy przetwarzanie danych opiera się na innej podstawie, pozyskiwanie zgody od osoby, której dane dotyczą jest zbędne. Podkreślił przy tym, iż powołane powyżej przepisy dotyczące uprawnień Rzecznika Praw Pacjenta w związku z prowadzeniem postępowań w sprawach praktyk naruszających zbiorowe prawa pacjenta, nie powinny być interpretowane jako zezwalające na automatyczne pozyskiwanie przez ten podmiot danych tzw. szczególnie chronionych, tylko powinno być każdorazowo uzależnione od zakresu i celu przeprowadzanego postępowania. Nie wyklucza to jednak możliwości pozyskiwania przez ten organ informacji zindywidualizowanych, pod warunkiem, iż zakres pozyskiwanych danych jest adekwatny do celu, a także uzasadniony i niezbędny dla wyjaśniania istotnych wątpliwości w toku prowadzonej kontroli.

Kolejne pytanie dotyczyło **wniosku, jaki wystosował Urząd Skarbowy do Niepublicznego Zakładu Opieki Zdrowotnej odnośnie udostępnienia danych osobowych pacjenta**<sup>182</sup>. Dopuszczalność przetwarzania danych osobowych uzależniona jest od spełnienia jednej z przesłanek legalności takiego działania, określonych w przepisach art. 23 ust. 1 bądź art. 27 ust. 2 ustawy o ochronie danych osobowych. GODO podkreślił, że podstawę prawną dla udostępniania danych organom ścigania np. urzędowi skarbowemu, jako podmiotom prowadzącym postępowanie karne, w tym także karnoskarbowe, może stanowić art. 15 § 3 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.). Wspomniany przepis nakłada na wszystkie osoby prawne lub jednostki organizacyjne niemające osobowości prawnej, inne niż określone w § 2 tego przepisu, a także na osoby fizyczne, obowiązek udzielenia pomocy na wezwanie organów prowadzących postępowanie karne w zakresie i w terminie przez nie wyznaczonym, jeżeli bez tej pomocy przeprowadzenie czynności procesowej jest niemożliwe albo znacznie utrudnione. Pomoc

---

<sup>182</sup> DOLiS-035-550/12/20924

ta ogranicza się wyłącznie do procesu karnego, ale rozumianego szeroko - począwszy od postępowania sprawdzającego, lecz z wyłączeniem czynności operacyjno-rozpoznawczych<sup>183</sup>. Podmiot występujący o udostępnienie określonych informacji powinien w sposób prawidłowy wskazać podstawę prawną upoważniającą go do uzyskania danych. 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 Urzędu Skarbowego z prośbą o wyjaśnienie tych wątpliwości. Generalny Inspektor podkreślił, że o udostępnieniu danych osobowych każdorazowo decyduje podmiot, do którego skierowano wniosek o udostępnienie danych osobowych po dokonaniu oceny, czy wskazana podstawa rzeczywiście uprawnia wnioskodawcę do pozyskania danych. Zdaniem Generalnego Inspektora, zarówno podmiot żądający udostępnienia danych osobowych – zwłaszcza jeśli jego działania są ściśle wyznaczone normami kompetencyjnymi – jak i udostępniający te dane, muszą mieć ku temu stosowną podstawę prawną. Administrator danych, dokonując tej czynności na danych osobowych, powinien być w stanie udowodnić, że udostępnia dane podmiotowi do tego uprawnionemu. Stosując w swej działalności zasady ochrony danych osobowych, administrator danych powinien dopełniać obowiązku dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, wynikających z art. 26 ust. 1 pkt 1-4 ustawy o ochronie danych osobowych. Generalny Inspektor uznał, iż zważywszy na jego kompetencje określone przepisami ustawy, nie jest on władny do ingerowania w postępowania prowadzone przez uprawnione do tego organy w trybie i na zasadach przewidzianych przepisami prawa. Podobne stanowisko zajął Naczelny Sąd Administracyjny, który w uzasadnieniu do wyroku z dnia 21 listopada 2000 r. w sprawie o sygn. akt II SA 308/00 stwierdził, iż „*ingerencja Generalnego Inspektora Ochrony Danych Osobowych w tok postępowania karnego jest niedopuszczalna, gdyż w przeciwnym razie zostałaby naruszona zasada wyłącznej kompetencji organów ścigania do prowadzenia postępowania przygotowawczego i niezawisłego sądu do wyłącznego sprawowania wymiaru sprawiedliwości*”. Generalny Inspektor przyznał wprawdzie, że wyrok ten dotyczy *stricte* postępowania karnego i ingerencji Generalnego Inspektora w jego tok, niemniej jednak stanowi on wskazówkę interpretacyjną, mającą przełożenie również na innego rodzaju ustawowo regulowane postępowania, do prowadzenia których właściwe są inne organy. Co więcej, Generalny Inspektor Ochrony Danych Osobowych nie może oceniać działań tych organów, co potwierdza Naczelny Sąd Administracyjny w wyroku z dnia 2 marca 2001 r. (sygn. akt II SA 401/00) stwierdzając, że „*(...) Generalny Inspektor (...) nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji, czy w inny sposób określony odpowiednimi procedurami*”.

---

<sup>183</sup> por. Kodeks postępowania karnego. Komentarz. Warszawa 2008, Wydawnictwo Prawnicze LexisNexis.

W dalszym ciągu wiele kierowanych w 2012 r. do Generalnego Inspektora zapytań dotyczyło **postępowania z dokumentacją medyczną**. W tym zakresie w odpowiedziach wskazywano na konieczność odwołania się do regulacji prawnych zawartych m.in. w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.) oraz rozporządzeniu Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz. U. Nr 247, poz. 1819). Z przepisów powołanych aktów prawnych wynika bowiem obowiązek tworzenia i przechowywania dokumentacji medycznej przez podmiot udzielający świadczeń zdrowotnych. Powyższe przepisy określają również zasady i sposób udostępniania dokumentacji medycznej wskazując, jakim podmiotom i w jakich celach dokumentacja ta może być udostępniana. I tak, podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta, dopuszczając jednakże wyjątki od tej zasady przewidujące możliwość udostępniania jej organom władzy publicznej (np. policji) w zakresie niezbędnym do wykonywania przez te podmioty ich zadań (art. 26 ust 3 pkt. 2). Zgodnie z art. 26 ust. 3 pkt 1 powołanej ustawy, podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną również podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych.

W kierowanych do GIODO pytaniach wątpliwości budziła również **kwestia dostępu do danych o stanie zdrowia przez zakłady ubezpieczeń**. Tutaj zastosowanie znajdują przepisy ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. z 2010 r. Nr 11, poz. 66 z późn. zm.). Zgodnie z art. 12 ust. 1 tej ustawy, zakład ubezpieczeń udziela ochrony ubezpieczeniowej na podstawie umowy ubezpieczenia zawartej z ubezpieczającym. Umowa ta ma charakter dobrowolny, z zastrzeżeniem przepisów ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych. Ogólne warunki ubezpieczenia oraz umowa ubezpieczenia powinny być formułowane jednoznacznie i w sposób zrozumiały (ust. 2 i 3).

Art. 15 ww. ustawy stanowi, że zakład ubezpieczeń wypłaca odszkodowanie lub świadczenie na podstawie uznania roszczenia uprawnionego z umowy ubezpieczenia, w wyniku ustaleń dokonanych w postępowaniu, o którym mowa w art. 16, zawartej z nim ugody lub prawomocnego orzeczenia sądu. Po otrzymaniu zawiadomienia o zajściu zdarzenia losowego objętego ochroną ubezpieczeniową, w terminie 7 dni od dnia otrzymania tego zawiadomienia, zakład ubezpieczeń informuje o tym ubezpieczającego lub ubezpieczonego, jeżeli nie są oni osobami występującymi z tym zawiadomieniem, oraz rozpoczyna postępowanie dotyczące ustalenia stanu faktycznego zdarzenia, zasadności zgłoszonych roszczeń i wysokości świadczenia, a także informuje osobę występującą z roszczeniem pisemnie lub w inny sposób, na który osoba ta wyraziła zgodę, jakie dokumenty są

potrzebne do ustalenia odpowiedzialności zakładu ubezpieczeń lub wysokości świadczenia, jeżeli jest to niezbędne do dalszego prowadzenia postępowania (art. 16 ust. 1). Stosownie do ust. 4 zakład ubezpieczeń ma obowiązek udostępniać osobom, o których mowa w ust. 1, oraz poszkodowanemu lub uprawnionemu, informacje i dokumenty gromadzone w celu ustalenia odpowiedzialności zakładu ubezpieczeń lub wysokości świadczenia. Osoby te mogą żądać pisemnego potwierdzenia przez zakład ubezpieczeń udostępnionych informacji, a także sporządzenia na swój koszt kserokopii dokumentów i potwierdzenia ich zgodności z oryginałem przez zakład ubezpieczeń. Informacje i dokumenty zakład ubezpieczeń ma obowiązek udostępniać osobom, o których mowa w ust. 1, oraz poszkodowanemu lub uprawnionemu, na ich żądanie, w postaci elektronicznej. W odpowiedziach na zapytania dotyczące podstaw przetwarzania danych o stanie zdrowia przez ubezpieczycieli wskazywano również, że zakład ubezpieczeń i osoby w nim zatrudnione lub osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia (art. 19 ust. 1 ustawy).

### 7.1.2. Banki i inne instytucje finansowe oraz firmy windykacyjne

Nadawcą jednego z pytań dotyczących windykacji był Departament Konsularny Ministerstwa Spraw Zagranicznych, który miał wątpliwości, **czy polska placówka konsularna może udostępniać dane adresowe obywateli polskich mieszkających w Irlandii, o które zwracają się firmy zajmujące się windykacją wierzytelności**<sup>184</sup>. Generalny Inspektor wskazał, że podstawą działalności podmiotów publicznych, jest zasada legalizmu, wynikająca z art. 7 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którą każde działanie administratora danych będącego podmiotem publicznym powinno mieć podstawę w obowiązujących przepisach prawa. W odniesieniu do podmiotów prywatnych obowiązuje odmienna zasada - podmioty te mogą podejmować wszelkie działania, których prawo im nie zabrania. Zestawienie wskazanych powyżej zasad ukazuje, iż zróżnicowanie sytuacji administratorów danych w pewnych sytuacjach znajduje uzasadnienie. Dopuszczenie możliwości przetwarzania danych osobowych przez administratorów danych ze sfery publicznej, w oparciu o inną, niż przepisy prawa, przesłankę, np. na podstawie tzw. klauzuli usprawiedliwionego celu, wynikającej z art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, może stwarzać zagrożenie, że podmioty te będą przetwarzać dane nie mając ku temu wyraźnych podstaw prawnych, a zatem z pominięciem wyżej przytoczonej, konstytucyjnej zasady legalizmu<sup>185</sup>. Natomiast podstawę przetwarzania danych osobowych przez konsułów Rzeczypospolitej Polskiej winna stanowić przesłanka wskazana w art. 23 ust. 1 pkt 2 lub – odpowiednio – art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, w związku

---

<sup>184</sup> DOLiS-035-1261/12/39941

<sup>185</sup> J. Barta, P. Fajgielski, R. Markiewicz, Ochrona Danych Osobowych, Komentarz, Wydanie 4, Kraków 2007, s. 467.

m.in. z przepisami ustawy z dnia 13 lutego 1984 r. o funkcjach konsułów Rzeczypospolitej Polskiej (t.j. Dz. U. z 2002 r. Nr 215, poz. 1823 z późn. zm.). Z przytoczonych przepisów wynika, że przetwarzanie danych osobowych jest dopuszczalne, jeżeli jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa. Przy czym w odniesieniu do danych szczególnie chronionych (katalog których zawarty został w art. 27 ust. 1 ustawy o ochronie danych osobowych) ustawodawca wymaga, by był to przepis rangi ustawy, stwarzający pełne gwarancje ochrony danych. W ocenie Generalnego Inspektora istotnym pozostaje również okoliczność, iż na podmiocie będącym administratorem danych, w sytuacji pozyskania przez niego danych osobowych w określonych, wynikających z przepisów prawa, celach, spoczywa co do zasady obowiązek niepoddawania zebranych danych dalszemu przetwarzaniu, niezgodnemu z tymi celami (art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych). Innymi słowy, przetwarzanie przez placówkę konsularną danych osobowych powinno następować w takich celach, jakie wynikają z obowiązujących przepisów prawa, dla jakich placówka dane te pozyskała.

Generalny Inspektor rozważał również problem dotyczący tego, **czy bank miał prawo dysponować danymi osobowymi skarżącego i przekazać je następnie do prokuratury rejonowej oraz to, czy miał prawo sprzedać dług skarżącego firmie windykacyjnej.**<sup>186</sup> W odpowiedzi Generalny Inspektor wskazał, że nie jest on organem uprawnionym do ingerowania w tok postępowania sądowego, w tym także postępowania karnego przygotowawczego. Argumentując powyższe powołał cytowane wcześniej orzeczenie Naczelnego Sądu Administracyjnego z dnia 21 listopada 2000 r. w sprawie o sygn. akt II SA 308/00. Generalny Inspektor nie jest też organem powołanym do ścigania przestępstw, w tym również tych określonych w przepisach karnych ustawy o ochronie danych osobowych. Leży to bowiem w gestii wyłącznie uprawnionych organów ścigania (policji, prokuratury), które dysponują szerokimi instrumentami prawnymi w tym zakresie. Podobnie Naczelny Sąd Administracyjny w wyroku z dnia 2 marca 2001 r. (sygn. akt II SA 401/00) stwierdził, że „(...) *Generalny Inspektor (...) nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji, czy w inny sposób określony odpowiednimi procedurami*”. Natomiast przetwarzanie danych osobowych przez firmę trudniącą się windykacją należności może opierać się o przesłankę wskazaną w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, zgodnie z którą przetwarzanie jest dopuszczalne, jeśli jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych lub odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Stosownie do art. 23 ust. 4 pkt 2 ustawy, za prawnie usprawiedliwiony cel uważa się dochodzenie

---

<sup>186</sup> DOLiS-035-1684/12/44748



roszczeń z tytułu prowadzonej przez administratora danych działalności gospodarczej. Rozstrzygającym wątpliwości dotyczące legalności przetwarzania danych w związku z cesją wierzytelności, jest wyrok Naczelnego Sądu Administracyjnego z dnia 6 czerwca 2005 r. (sygn. akt I OPS 2/2005), z którego wynika, że można przekazywać firmom windykacyjnym dane dłużników bez ich zgody, jednakże trzeba odpowiednio wyważyć między ochroną praw i wolności obywatelskich a interesami wierzycieli. Ponadto administrator danych może także powierzyć firmie windykacyjnej przetwarzanie danych osobowych w trybie i na zasadach określonych w art. 31 ustawy. W takiej sytuacji zarówno obowiązki administratora danych, jak i podmiotu, któremu powierzono przetwarzanie danych oraz ich szczegółowy zakres, powinno być określone w zawartej między nimi umowie. Podmiot, któremu na podstawie ww. umowy administrator danych powierzył przetwarzanie danych, może je przetwarzać wyłącznie w zakresie i w celu przewidzianym w tej umowie (ust. 2 art. 31 ustawy). W świetle art. 509 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.), wierzyciel może bez zgody dłużnika przenieść wierzytelności na osobę trzecią (przelew), chyba, że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania (§ 1). Wraz z wierzytelnością przechodzą na nabywcę wszelkie związane z nią prawa, w szczególności roszczenie o zaległe odsetki (§ 2 ww. przepisu). Jak zauważył Generalny Inspektor, przepisy nie określają sposobu i procedury weryfikacji klienta przez firmę windykacyjną, a każdy podmiot przetwarzający dane osobowe powinien w taki sposób zabezpieczać dane, w tym weryfikować klienta, aby jego dane osobowe nie zostały udostępnione osobom nieupoważnionym. Osobną kwestią było badanie zasadności dochodzenia roszczeń przez określony podmiot. Niemniej jednak rozstrzyganie wszelkich zagadnień spornych, dotyczących niewykonania lub nienależytego wykonania zobowiązań, należy do wyłącznej kompetencji sądu cywilnego, a nie do organu do spraw ochrony danych osobowych, co potwierdził przywołany już wcześniej wyrok Naczelnego Sądu Administracyjnego z dnia 2 marca 2001 r. (sygn. akt II SA 401/00).

Kolejne istotne pytanie dotyczyło **podstawy prawnej występowania do BIK o BANKOWY RAPORT - ZARZĄDZANIE KLIENTEM INDYWIDUALNYM dla celów tworzenia zindywidualizowanej oferty usług bankowych**<sup>187</sup>. W odpowiedzi Generalny Inspektor przywołał treść art. 12 ustawy o ochronie danych osobowych i wskazał, że zakres przedmiotowych kompetencji nie zobowiązuje organu do spraw ochrony danych osobowych do udzielania porad i sporządzania opinii prawnych w sprawach sygnalizowanych w kierowanych do niego pismach. W przedmiocie oceny legalności procesu przetwarzania danych osobowych, Generalny Inspektor może wiążąco wypowiedzieć się wyłącznie po przeprowadzeniu postępowania w sprawie dotyczącej procesu przetwarzania danych, na podstawie poczynionych w jego toku ustaleń i z uwzględnieniem

---

<sup>187</sup> DOLiS-035-1142/13/49672/12

obowiązujących, przepisów prawa. Niezależnie od powyższego wskazał, że każde przetwarzanie danych osobowych powinno znajdować stosowną podstawę prawną, czyli pozostawać w zgodzie z powszechnie obowiązującymi przepisami prawa. Problematykę przetwarzania danych osobowych przez biura informacji kredytowej regulują przepisy ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 7, poz. 665 z późn. zm.). Na podstawie art. 105 ust. 4 ww. ustawy, banki mogą tworzyć instytucje upoważnione do gromadzenia, przetwarzania i udostępniania innym bankom informacji stanowiących tajemnicę bankową w zakresie, w jakim informacje te są potrzebne w związku z wykonywaniem czynności bankowych, a także innym instytucjom ustawowo upoważnionym do udzielania kredytów – informacji stanowiących tajemnicę bankową w zakresie, w jakim informacje te są niezbędne w związku z udzielaniem kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń. Podstawowymi celami wspomnianych biur jest opracowywanie informacji kredytowych na potrzeby banków, zmniejszanie ryzyka związanego z udzieleniem kredytu, uproszczenie i przyspieszenie procedur udzielania kredytu, zmniejszenie kosztów obsługi kontrahenta bankowego, poprawa konkurencyjności banków polskich, zwiększenie bezpieczeństwa obrotu kredytowego. Zdaniem Generalnego Inspektora przekazywanie przez banki danych osobowych osób fizycznych do biur informacji kredytowych w celu pozyskania informacji o sytuacji finansowej konkretnych osób na potrzeby realizacji wobec nich skuteczniejszego marketingu, stanowi więc naruszenie zasad określonych ww. przepisach, a tym samym nie może być uznane za zgodne z zasadami ochrony danych osobowych. Cele, dla których banki mogą zarówno udostępniać, jak i pozyskiwać dane z biur informacji kredytowej są bowiem jednoznacznie określone w ustawie Prawo bankowe. Tylko we wskazanych przez ustawodawcę sytuacjach, banki mogą przetwarzać dane osobowe za pośrednictwem tych instytucji. Generalny Inspektor dodał również, że dane osobowe osoby, która „nie złożyła żadnego wniosku o kartę, ani o inny produkt kredytowy, ani też nie posiada w banku żadnego produktu kredytowego” mogą być przetwarzane w celach marketingowych wyłącznie za jej wyraźną zgodą.

Część zapytań dotyczących działalności banków odnosiło się do **naruszeń tajemnicy bankowej**<sup>188</sup>. W takich przypadkach Generalny Inspektor wskazywał właściwe regulacje prawne w tym zakresie oraz informował, że jeśli określone działania wypełniają znamiona czynu karalnego, to należy skierować zawiadomienie do właściwych organów ścigania. Mocą art. 171 ust. 5 Prawa bankowego, kto będąc obowiązany do zachowania tajemnicy bankowej, ujawnia lub wykorzystuje informacje stanowiące tajemnicę bankową, niezgodnie z upoważnieniem określonym w ustawie, podlega grzywnie do 1.000.000 złotych i karze pozbawienia wolności do lat 3. Ponadto zgodnie z art. 51 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia

---

<sup>188</sup> np. DOLiS-035-3213/12

dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Podobnie jak w poprzednich okresach sprawozdawczych, w 2012 r. organowi do spraw danych osobowych nadal zgłaszane były zastrzeżenia i wątpliwości dotyczące **dopuszczalności kopiowania dowodów tożsamości w związku z korzystaniem z usług bankowych**<sup>189</sup>. W odpowiedzi Generalny Inspektor wskazywał, że kwestia ta jest przedmiotem szczególnych regulacji ustawowych, które znajdują tutaj bezpośrednie zastosowanie. Zgodnie z art. 112b ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t. j. Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm) banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych. Uprawnienie zawarte w tym przepisie uzasadniane jest szczególnym statusem banków, jako instytucji zaufania publicznego i ich szczególnymi obowiązkami realizowanymi dla celów społecznych. Podkreślał też, że sposób pozyskiwania danych osobowych z punktu widzenia przepisów ustawy o ochronie danych osobowych nie ma znaczenia, o ile dane te przetwarzane są w zakresie adekwatnym do celu przetwarzania, tym bardziej gdy zakres przetwarzanych danych regulują stosowne przepisy prawa – w tym przypadku art. 112b Prawa bankowego. Warto również mieć na uwadze, że Naczelny Sąd Administracyjny w wyroku z dnia 19 grudnia 2001 r. (sygn. akt II SA 2869/00) orzekł: „(...) *gromadzenie danych osobowych przez wykonanie kopii dokumentu zawierającego te dane jest kwestią techniczną, obojętną dla prawodawcy reglamentującego w ustawie o ochronie danych osobowych przetwarzanie tego rodzaju danych. Inaczej mówiąc posługiwanie się taką czy inną techniką utrwalania danych (kopiowanie lub przepisywanie) nie przesądza samo przez się o legalności tego utrwalania (przetwarzania). Dla takich ocen istotne znaczenie mają przede wszystkim: podstawa prawna przetwarzania danych (art. 23 ustawy), rodzaj przetwarzanych danych (art. 27) oraz granice przetwarzania (art. 26 ust. 1 pkt 3)*”. Analogiczne stanowisko zajął Naczelny Sąd Administracyjny w wyroku z dnia 7 listopada 2003 r. (sygn. akt II SA 1432/02) stanowiącym, że „ustawa o ochronie danych osobowych nie zajmuje się określaniem techniki gromadzenia danych osobowych lecz zakresem ich przetwarzania (...)”. Kopiowanie, czy skanowanie dokumentów zawierających dane osobowe nie będzie więc niezgodne z prawem, jeśli nie będzie prowadziło do gromadzenia danych w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są przetwarzane (ww. zasada adekwatności).

Interesująca była także odpowiedź na pytanie nadesłane z Kancelarii Prezesa Rady Ministrów odnośnie **zasadności pytania o stan cywilny przy zawieraniu umowy ubezpieczenia AC/OC oraz kredytu bankowego**. W odpowiedzi<sup>190</sup> Generalny Inspektor wskazał, że podstawowymi przepisami

---

<sup>189</sup> np. DOLiS-035- 2266/11

<sup>190</sup> DOLiS-035-3147/12/1379/12

określającymi zasady odpowiedzialności gwarancyjnej zakładu ubezpieczeń z tytułu obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych są przepisy ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. z 2003 r. Nr 124, poz. 1152 z późn. zm.), a także przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.). Generalny Inspektor zwrócił również uwagę na art. 24 ust. 1 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. z 2010 r. Nr 11, poz. 66 z późn. zm.).<sup>191</sup> Zastrzegł jednocześnie, że kwestię zakresu danych pozyskiwanych przez zakład ubezpieczeń dla celów ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych za szkody powstałe w związku z ruchem tych pojazdów oraz ubezpieczenia casco, w tym informacji o stanie cywilnym, należałoby oceniać *in concreto*, z uwzględnieniem celu, dla którego informacja ta jest pozyskiwana, a zatem w kontekście zasady adekwatności określonej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Zwrócił też uwagę na wyrok NSA z dnia 5 lutego 2003 r. (sygn. akt II SA 3505/01), w którym Naczelny Sąd Administracyjny potwierdził konieczność badania celu pozyskiwania danych określonego rodzaju przy dokonywaniu oceny respektowania zasady celowości i adekwatności gromadzenia danych. Generalny Inspektor poinformował, że zbadanie tej kwestii i wydanie w tym przedmiocie wiążącego rozstrzygnięcia wobec określonego zakładu ubezpieczeń mogłoby nastąpić jedynie po przeprowadzeniu postępowania administracyjnego w decyzji administracyjnej. Tylko w takim postępowaniu Generalny Inspektor może ustalić, czy w związku z przetwarzaniem danych osobowych konkretnej osoby doszło do naruszenia przepisów prawa, w tym zasady adekwatności. Skargę lub wniosek w określonej sprawie może złożyć osoba, która uznaje, że ochrona jej danych osobowych została naruszona, lub która domaga się przywrócenia stanu zgodnego z prawem, w stosunku do jej danych osobowych. Przy czym postępowanie administracyjne może być zainicjowane jedynie taką skargą lub wnioskiem, które spełniają wymogi formalne - zgodnie z przepisami Kodeksu postępowania administracyjnego (art. 63) oraz ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz. U. Nr 225, poz. 1635 z późn. zm.). W uzupełnieniu powyższych uwag Generalny Inspektor wskazał, że ustawa o ochronie danych zobowiązuje każdego administratora danych do przestrzegania zasady celowości, wyrażającej się w obowiązku precyzyjnego i ścisłego określenia celu przetwarzania określonego rodzaju danych (np. o stanie cywilnym). Dokonanie przez administratora danych rzetelnej analizy, czy i dla jakich celów pozyskiwanie określonego rodzaju danych jest w istocie niezbędne, powinno następować na etapie poprzedzającym gromadzenie danych. Generalny Inspektor podniósł, że tylko takie podejście warunkuje prawidłowe respektowanie przez administratora danych, zasad wyrażonych

---

<sup>191</sup> Zakład ubezpieczeń może zbierać, odpowiednio w celu oceny ryzyka ubezpieczeniowego lub wykonania umowy ubezpieczenia, zawarte w umowach ubezpieczenia lub oświadczeniach ubezpieczających składanych przed zawarciem umowy ubezpieczenia, dane ubezpieczonych lub uprawnionych z umowy ubezpieczenia.

w ustawie o ochronie danych osobowych: zasady związania celem (art. 26 ust. 1 pkt 2 ustawy), zasady adekwatności danych do celu przetwarzania (art. 26 ust. 1 pkt 3 ustawy), czy zasady ograniczenia czasowego przetwarzania (art. 26 ust. 1 pkt 4 ustawy). Zdaniem Generalnego Inspektora, rzetelne przestrzeganie powyższych zasad stanowi również gwarancje właściwego poszanowania praw osób, których dane dotyczą. Cytując art. 26 ust. 1 ustawy o ochronie danych osobowych podkreślił, że zasada celowości przetwarzania danych osobowych polega więc na tym, że administrator danych może je przetwarzać jedynie w celach realizacji zadań lub wykonywania udzielonych mu kompetencji. Zaznaczył jednocześnie, że cel przetwarzania danych osobowych nie jest wynikiem arbitralnej decyzji oderwanym od okoliczności przetwarzania. Ustalając cel należy odwołać się do kontekstu przetwarzania. Swoim rodzajem oraz treścią dane osobowe nie powinny wykraczać poza potrzeby wynikające z celu ich przetwarzania. Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane (wyrok Wojewódzkiego Sądu Administracyjnego z dnia 1 grudnia 2005 roku, sygn. II SA/Wa 917/2005). W drugiej części wystąpienia Generalny Inspektor poinformował, że podstawą do przetwarzania danych osobowych przez banki w ramach działalności kredytowej są przepisy ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe oraz wydane na jej podstawie akty wykonawcze. W szczególności zwrócił uwagę na treść art. 70 ust. 1-2 ww. aktu prawnego<sup>192</sup>. Ponadto powołał treść art. 112b prawa bankowego<sup>193</sup>. W świetle powyższego Generalny Inspektor stwierdził, że z regulacji powołanego art. 70 wynika obowiązek banku zbadania zdolności kredytowej podmiotu ubiegającego się o kredyt. Zastrzegł jednak, iż powołany przepis prawa bankowego nie wskazuje wprost, jakie dokumenty oraz w jakim zakresie powinny być podstawą do oceny zdolności kredytowej. Dlatego też bank również powinien stosować dla potrzeb oceny tej zdolności - wskazane powyżej - zasady wynikające z art. 26 ustawy o ochronie danych osobowych. Wyjaśnił też, że przepisy art. 32-35 rozdziału 4 ustawy o ochronie danych osobowych, określają katalog uprawnień przysługujących osobie fizycznej, której dane dotyczą, w zakresie kontroli procesu przetwarzania jej danych w zbiorach danych przez administratora danych. Kontrola tego procesu powinna być w pierwszej kolejności dokonywana na wniosek osoby, której dane dotyczą, złożony do administratora danych. Osoba taka może zwrócić się do administratora danych z pytaniem dotyczącym uzasadnienia prawnego i faktycznego (czyli celu) pozyskiwania określonego rodzaju danych osobowych.

---

<sup>192</sup> Banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych.

<sup>193</sup> Banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych.

Kolejne istotne pytanie dotyczyło **żądania numeru PESEL przy dokonywaniu płatności internetowej**. W odpowiedzi<sup>194</sup> Generalny Inspektor wskazał, że ustawa o ochronie danych osobowych określa ogólne zasady przetwarzania i ochrony danych osobowych, zaś ich skonkretyzowanie ma miejsce w szczególnych wobec jej uregulowań przepisach prawa. W sytuacji, gdy określone zagadnienia są przedmiotem regulacji innych aktów prawnych, należy się dowołać także do nich (art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych). Jeżeli zatem inne, szczególne przepisy prawa, przyznają konkretnemu podmiotowi uprawnienie do przetwarzania danych osobowych w zakresie m.in. numeru PESEL, ustawa o ochronie danych osobowych, co do zasady, nie stoi temu na przeszkodzie. Generalny Inspektor podniósł, że kwestie dotyczące realizacji płatności internetowych z użyciem kart kredytowych należałoby rozpatrywać m.in. na gruncie przepisów ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.) oraz ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. Nr 169, poz. 1385 z późn. zm.). W myśl art. 8b ust. 1 i 3 pkt 1 pierwszego z przywołanych aktów prawnych, instytucje obowiązane (do których należą m.in. instytucje pieniądza elektronicznego, oddziały zagranicznych instytucji pieniądza elektronicznego oraz agenci rozliczeniowi prowadzący działalność na podstawie ustawy o elektronicznych instrumentach płatniczych) stosują wobec swoich klientów środki bezpieczeństwa finansowego. Zakres stosowania jest określany na podstawie oceny ryzyka prania pieniędzy i finansowania terroryzmu, dokonanej w wyniku analizy, z uwzględnieniem w szczególności rodzaju klienta, stosunków gospodarczych, produktów lub transakcji. Środki bezpieczeństwa finansowego, o których mowa w ust. 1, polegają na identyfikacji klienta i weryfikacji jego tożsamości na podstawie dokumentów lub informacji publicznie dostępnych (art. 8b ust. 3 pkt 1). Identyfikacja, o której mowa w art. 8b ust. 3 pkt 1, obejmuje zaś – w przypadku osób fizycznych i ich przedstawicieli – ustalenie i zapisanie cech dokumentu stwierdzającego na podstawie odrębnych przepisów tożsamość osoby, a także imienia, nazwiska, obywatelstwa oraz adresu osoby dokonującej transakcji, a ponadto numeru PESEL lub daty urodzenia w przypadku osoby nieposiadającej numeru PESEL, lub numeru dokumentu stwierdzającego tożsamość cudzoziemca, lub kodu kraju w przypadku przedstawienia paszportu (art. 9 ust. 1 pkt 1 ustawy). Jak zauważył Generalny Inspektor, z punktu widzenia przepisów o ochronie danych osobowych istotne pozostaje, aby przetwarzane dane osobowe były adekwatne w stosunku do celu ich przetwarzania (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). 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 (wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r. o sygn. akt II SA/Wa 917/2005). Generalny

---

<sup>194</sup> DOLIS-035-1877/12

Inspektor podkreślił, że jeżeli celem przetwarzania danych (ich pozyskiwania) jest np. identyfikacja konkretnej osoby, z punktu widzenia przepisów o ochronie danych osobowych dopuszczalnym pozostaje pozyskiwanie takiego zakresu danych, jaki będzie wystarczający do dokonania bezbłędnej identyfikacji osoby – w tym przypadku – klienta, umożliwiającej w konsekwencji prawidłowe wykonywanie przepisów innych ustaw – w tym przypadku ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.

### 7.1.3. Przetwarzanie danych osobowych – wybrane problemy

Interesujące zagadnienie z punktu widzenia ochrony danych osobowych zawarte było w pytaniu, **czy każdy członek rady gminy ma prawo wglądu do danych osobowych osób korzystających ze świadczeń pomocy społecznej**. W odpowiedzi<sup>195</sup> Generalny Inspektor wskazał, że przetwarzanie danych osobowych w każdym przypadku powinno się odbywać z poszanowaniem zasad wynikających z powszechnie obowiązujących przepisów prawa, w tym przepisów ustawy o ochronie danych osobowych i wydanych na jej podstawie aktów wykonawczych. Jeśli natomiast istnieją szczególne przepisy, to stosuje się je w pierwszej kolejności. Dopiero w sytuacji braku tych przepisów, zastosowanie znajduje ogólna regulacja wynikająca z ustawy o ochronie danych osobowych. Generalny Inspektor pomocniczo wskazał, iż zgodnie z art. 18a ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.), rada gminy kontroluje działalność wójta, gminnych jednostek organizacyjnych oraz jednostek pomocniczych gminy i w tym celu powołuje komisję rewizyjną. Ponadto 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). Jakkolwiek wyżej wymienione przepisy ustawy o samorządzie gminnym stwarzają podstawy do utworzenia w gminie komisji rewizyjnej, to - jak zauważył Generalny Inspektor - przepisy te nie określają 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. Generalny Inspektor wysnuł jednak wniosek, że ewentualny dostęp do danych osób korzystających ze świadczeń z zakresu pomocy społecznej może mieć komisja rewizyjna w ramach przeprowadzanej kontroli, w której zakres będzie wchodziło uprawnienie do zapoznania się z danym dokumentem. Przypomniał również, że ustawa o ochronie danych osobowych – jako, że w żadnym jej przepisie ustawodawca nie reguluje zasad posługiwania się dokumentami - nie ma zastosowania do udostępniania dokumentów, a jedynie do

---

<sup>195</sup> DOLiS-035-730/12/26590

wykonywania operacji na danych osobowych. Stanowisko takie zajął Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 10 października 2005 r. wydanym w sprawie o sygnaturze akt: II SA/Wa 825/2005, orzekając, że w ustawie o ochronie danych osobowych brak jest przepisów obligujących administratora do udostępnienia dokumentów zawierających dane osobowe. Ustawodawca posługuje się pojęciem „udostępnienia”, odnosząc je zawsze do danych osobowych, a nie do zawierających je dokumentów. Wskazał jednocześnie, iż dane osób korzystających ze świadczeń z zakresu pomocy społecznej stanowią dane szczególnie chronione, które ustawa o ochronie danych osobowych zabrania - co do zasady - przetwarzać (art. 27 ust. 1 ustawy o ochronie danych osobowych). Dane szczególnie chronione mogą być przetwarzane po spełnieniu jednej z przesłanek legalizujących ten proces, określonej w art. 27 ust. 2 pkt 1 - pkt 10 ustawy o ochronie danych osobowych. Przesłanki te mają charakter autonomiczny i rozłączny. Spełnienie jednej z nich wystarczy dla uznania legalności przetwarzania danych osobowych. Generalny Inspektor przypomniał również, że ostateczne rozstrzygnięcie w przedmiocie, czy udostępnić posiadane dane osobowe w zakresie żądanym przez występującego o to potencjalnego odbiorcę danych, należy do administratora danych. Dokonując takiego rozstrzygnięcia administrator powinien uwzględnić obowiązki, jakie w zakresie przetwarzania danych nakładają na niego przepisy o ochronie danych osobowych. Ich naruszenie może narazić administratora danych zarówno na odpowiedzialność administracyjną przed Generalnym Inspektorem Ochrony Danych Osobowych, jak i karną wynikającą z przepisów ustawy o ochronie danych osobowych.

Generalny Inspektor odpowiedział również na pytanie dotyczące **udostępniania rodzinnego wywiadu środowiskowego przeprowadzonego z klientem pomocy społecznej na potrzeby sądu**. W odpowiedzi<sup>196</sup> wskazał, iż nie jest możliwe zajęcie przez Generalnego Inspektora Ochrony Danych Osobowych wiążącego stanowiska w sprawie oraz dokonanie przez ten organ interpretacji treści obowiązujących aktów prawnych, poza toczącym się postępowaniem administracyjnym, w innej formie, aniżeli decyzja administracyjna. Jedynie informacyjnie wskazał, iż ustawa o ochronie danych osobowych określa ogólne zasady przetwarzania i ochrony danych osobowych, zaś ich skonkretyzowanie ma miejsce w szczególnych wobec jej uregulowań przepisach prawa. W sytuacji, gdy określone zagadnienia uregulowane zostały w przepisach innych aktów prawnych, należy się do nich odwołać (art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych). Jak zauważył Generalny Inspektor, kwestie dotyczące prowadzenia przez sąd postępowania sądowego w sprawach m.in. ze stosunków z zakresu prawa cywilnego, rodzinnego i opiekuńczego oraz prawa pracy, jak również w sprawach z zakresu ubezpieczeń społecznych, są w szczególności przedmiotem regulacji przepisów ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43,

---

<sup>196</sup> DOLiS-035-2452/12/5897



poz. 296 z późn. zm.). Zgodnie z art. 248 ust. 1 znajdującym się w księdze I części I kodeksu, zatytułowanej „Postępowanie rozpoznawcze”, każdy obowiązany jest przedstawić na zarządzenie sądu, w oznaczonym terminie i miejscu, dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera informacje niejawne. § 2 ww. artykułu precyzuje, iż od przedmiotowego obowiązku może uchylić się ten, kto co do okoliczności objętych treścią dokumentu mógłby jako świadek odmówić zeznania, albo kto posiada dokument w imieniu osoby trzeciej, która mogłaby z takich samych przyczyn sprzeciwić się jego przedstawieniu. Jednakże i wówczas nie można odmówić przedstawienia dokumentu, gdy jego posiadacz lub osoba trzecia obowiązani są do tego względem chociażby jednej ze stron, albo gdy dokument wystawiony jest w interesie strony, która żąda przeprowadzenia dowodu. Strona nie może ponadto odmówić przedstawienia dokumentu, jeżeli szkoda, na którą byłaby przez to narażona, polega na przegraniu procesu.

Jednym z istotniejszych pytań nadesłanych do Biura Generalnego Inspektora Ochrony Danych Osobowych w analizowanym okresie było pytanie, czy **funkcjonariusz Służby Więziennej musi podawać w oświadczeniu majątkowym dochody żony**<sup>197</sup>. W odpowiedzi poinformowano, że odnośnie obowiązku podania w oświadczeniu majątkowym informacji o zarobkach małżonka osoby składającej to oświadczenie, na gruncie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, legalność przetwarzania (w tym np. zbierania) danych osobowych tzw. zwykłych (jak np. imię, nazwisko, informacje o posiadanym majątku) uzależniona jest od spełnienia jednej z przesłanek wymienionych w art. 23 ust. 1 pkt 1 – 5 ustawy. I tak, zgodnie z art. 23 ust. 1 pkt 2 ustawy, przetwarzanie danych jest dopuszczalne wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Mając powyższe na uwadze stwierdzono, iż przetwarzanie danych osobowych w przedstawionej sprawie znajduje swoje uzasadnienie w przepisach ustawy z dnia 9 kwietnia 2010 r. (Dz. U. z 2010 Nr 79, poz. 523 z późn. zm.) o Służbie Więziennej. Zgodnie z art. 161 ust. 1 przytoczonej ustawy, przy nawiązaniu stosunku służbowego funkcjonariusz jest obowiązany złożyć oświadczenie o swoim stanie majątkowym, obejmującym majątek stanowiący małżeńską wspólność majątkową i jego majątek osobisty, a następnie do dnia 31 marca każdego roku, według stanu na dzień 31 grudnia roku poprzedniego, a także przy rozwiązaniu stosunku służbowego. Zasady składania takiego oświadczenia określają pozostałe normy ust. 2-6 powołanego artykułu oraz stosowne inne przepisy prawa w nich wskazane. Jak zauważył Generalny Inspektor powyższy przepis przesądza, że składane oświadczenia majątkowe dotyczą zarówno majątku odrębnego, jak i majątku objętego małżeńską wspólnością majątkową. Do majątku wspólnego należą w szczególności, zgodnie z art. 31 § 2 ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy

---

<sup>197</sup> DOLiS-035- 530/12/21010

(Dz. U. z 1964 r. Nr 9, poz. 59 z późn. zm.): pobrane wynagrodzenie za pracę i dochody z innej działalności zarobkowej każdego z małżonków (ust. 1); dochody z majątku wspólnego, jak również z majątku osobistego każdego z małżonków (ust. 2); środki zgromadzone na rachunku otwartego lub pracowniczego funduszu emerytalnego każdego z małżonków (ust. 3) oraz kwoty składek zewidencjonowanych na subkoncie, o którym mowa w art. 40a ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2009 r. Nr 205, poz. 1585 z późn. zm.). Generalny Inspektor zwrócił uwagę, iż przesłanki legalizujące proces przetwarzania danych osobowych, zawarte w art. 23 ust. 1 ustawy, mają charakter równoprawny, co oznacza, że dla wykazania legalności takiego procesu wystarcza spełnienie jednej z nich. W związku z tym, że w niniejszej sprawie podstawę przetwarzania danych osobowych stanowią przepisy prawa – obowiązek przetwarzania danych osobowych nałożony został na obywatela przez ustawodawcę i stanowi wystarczająca przesłankę do przetwarzania przedmiotowych danych osobowych.

Do Generalnego Inspektora nadesłano również pytanie z Ministerstwa Kultury i Dziedzictwa Narodowego w sprawie **legalności wydania publikacji dotyczących strat wojennych prywatnych kolekcjonerów warszawskich obejmujące dane osobowe właścicieli utraconego mienia**. W odpowiedzi<sup>198</sup> Generalny Inspektor wskazał, że istotą ochrony danych osobowych jest ochrona prywatności osoby, której dane dotyczą. Źródło tej ochrony wynika przede wszystkim z przepisów Konstytucji RP. Generalny Inspektor zwrócił tutaj szczególną uwagę na treść art. 47 oraz art. 51 ust. 5 Konstytucji. Wskazał również stanowisko Sądu Najwyższego wyrażone w postanowieniu z dnia 11 grudnia 2000 r. o sygn. II KKN 438/2000, w którym Sąd ten stwierdził, iż *„Dane osobowe korzystają z ochrony przewidzianej ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych już wówczas, jeżeli tylko mogą znaleźć się w zbiorze danych osobowych, bez względu na to, czy się w nim ostatecznie znalazły, a ustawa w odniesieniu do różnych etapów i rodzajów przetwarzania danych, określa jeszcze dodatkowe uprawnienia osób, których dane te dotyczą (rozd. 4 ustawy). Rzecz bowiem w tym, że każdy ma prawo do ochrony dotyczących go danych osobowych (art. 1 ust. 1 ustawy), a nie jedynie ten, czyje dane znalazły się już w zbiorze”*. Ponadto zaznaczył, że z art. 3a ust. 2 ustawy o ochronie danych osobowych wynika, że powołanej ustawy, z wyjątkiem art. 14–19 i art. 36 ust. 1, nie stosuje się m.in. do działalności literackiej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą. W ustawie brak jest jednak definicji wyrażenia „działalność literacka”, co do której wyłączone jest stosowanie jej przepisów, jak również nie odsyła ona w tym zakresie do innych aktów prawnych. Generalny Inspektor uznał, że przez działalność literacką należy rozumieć w szczególności działalność twórczą będącą przedmiotem prawa autorskiego, zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie

---

<sup>198</sup> DOLiS-035-543/12/24442

autorskim i prawach pokrewnych (t. j. Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.). Jak wynika z art. 1 ust. 1 niniejszej ustawy, przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór); m.in. utwór wyrażony słowem. Generalny Inspektor uznał zatem, że rozstrzygnięcie przedstawionego zagadnienia sprowadza się w istocie do dokonania oceny, czy w sprawie tej zostaną spełnione warunki określone w art. 3a ust. 2 cytowanej ustawy, a zatem, czy publikacja poświęcona stratom wojennym prywatnych kolekcjonerów warszawskich będzie formą wykonywania działalności literackiej. Zdaniem Generalnego Inspektora, drugą obok wykonywania działalności literackiej przesłanką, którą wymienia art. 3a ust. 2 ustawy o ochronie danych osobowych i którą należałoby wziąć pod uwagę w niniejszej sprawie, jest okoliczność, że wolność wyrażania swoich poglądów i rozpowszechniania informacji nie może istotnie naruszać praw i wolności osoby, której dane dotyczą. Konkludując, według Generalnego Inspektora w sytuacji, gdy publikacja poświęcona stratom wojennym prywatnych kolekcjonerów warszawskich nie będzie spełniała przesłanek, o których mowa powyżej, wówczas administrator danych winien wypełnić wszelkie obowiązki, jakie nakłada na niego ustawa o ochronie danych osobowych. Z punktu widzenia przepisów o ochronie danych osobowych istotne jest przede wszystkim, aby czynność przetwarzania znajdowała podstawę w jednej z ustawowych przesłanek legalizacyjnych. W przypadku, gdy nie zachodzi żadna z tych podstaw (ustanowionych w pkt 2-5 art. 23 lub pkt 2-10 art. 27 ustawy o ochronie danych osobowych), jedyną właściwą podstawą udostępnienia danych osobowych właścicieli/kolekcjonerów warszawskich byłaby zgoda osoby, której te dane dotyczą. Generalny Inspektor podkreślił, iż zgodnie z art. 2 ust. 1 ustawy o ochronie danych osobowych, ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Generalny Inspektor przypomniał, że zgodnie z powszechnie obowiązującą wykładnią, osobą fizyczną jest człowiek uczestniczący w stosunkach prawnych. Zdolność prawna człowieka, a tym samym zdolność do bycia podmiotem praw i obowiązków, ustaje z chwilą jego śmierci. Osoba zmarła nie może być podmiotem praw i obowiązków w stosunkach prawnych i nie może być zatem uznana za osobę fizyczną, a więc jej dane osobowe nie są objęte ochroną z mocy przepisów ustawy o ochronie danych osobowych. Generalny Inspektor nadmienił, że rozumiejąc ideę polegającą na propagowaniu wiedzy na temat polskich start wojennych należy jednak rozważyć, czy wszelkie dane, a zwłaszcza pełny adres zamieszkania przed/podczas okupacji (ulica, numer domu) właściciela/kolekcjonera warszawskiego są niezbędne w przedmiotowej publikacji. Nie można bowiem wykluczyć, iż pomimo upływu czasu w niektórych przypadkach będzie to aktualny adres zamieszkania takiej osoby, co w połączeniu z informacjami na temat kolekcji, jakie dana osoba posiadała i ewentualnie straciła podczas wojny, może świadczyć o jej statusie majątkowym i narazić ją na niebezpieczeństwo. Jednocześnie Generalny Inspektor wskazał na konieczność przestrzegania

zasady adekwatności i przypomniał, że do wszelkiego rodzaju przedsięwzięć polegających na udostępnianiu danych osobowych nieokreślonemu kręgowi osób, należy podchodzić ze szczególną ostrożnością. W przypadku, udostępnienia danych w sieci Internet, ich wyeliminowanie z „sieci” może być niemożliwe w sposób trwały. Z tych względów niezwykle istotna jest ochrona prywatności w Internecie.

Interesujące było również pytanie z Ministerstwa Rozwoju Regionalnego w sprawie dotyczącej kwestii, **kto jest administratorem danych osobowych w związku przetwarzaniem danych osobowych przez Instytucje Pośredniczące lub Instytucje Wdrażające w ramach programów operacyjnych współfinansowanych z funduszy Unii Europejskich.** W odpowiedzi<sup>199</sup> Generalny Inspektor powołał definicję administratora danych wyrażoną w art. 7 pkt 4 tej ustawy o ochronie danych osobowych. Jednocześnie wskazał, iż w przypadku podmiotów publicznych mogą one decydować o celu przetwarzania danych osobowych w ramach zadań, jakie wykonują zgodnie z przepisami ustaw szczególnych, i które tymi przepisami zostały wyznaczone. Innymi słowy, rozstrzygnięcie, któremu podmiotowi działającemu w sektorze publicznym przysługuje status administratora danych, wymaga analizy przepisów prawa w oparciu, o które podmiot ten działa. Jak zauważył Generalny Inspektor, przypisanie statusu administratora danych osobowych jednemu z podmiotów uczestniczących w realizacji programów finansowanych ze środków Unii Europejskiej determinowane jest niejednokrotnie treścią podpisywanych porozumień i zawieranych umów, które określają szczegółowe zadania, zasady i warunki realizacji działań oraz uprawnienia i obowiązki stron, także w zakresie administrowania danymi osobowymi. Generalny Inspektor uznał, że aby wskazać administratora danych, a tym samym podmiot obowiązany do wypełniania wszelkich wymogów nałożonych na niego przepisami o ochronie danych osobowych, należy każdorazowo dokonać analizy zapisów zawartych w wyżej wskazanych dokumentach. Obowiązek przeprowadzenia takiej analizy ciąży zaś na podmiotach uczestniczących w przygotowaniu i realizacji określonych programów operacyjnych. Generalny Inspektor może zaś tylko dokonać weryfikacji poczynionych ustaleń, w toku prowadzonego postępowania administracyjnego, np. dotyczącego realizowania obowiązku rejestracji konkretnego zbioru danych osobowych, bądź w toku czynności kontrolnych. Nadmienił też, iż Grupa Robocza Art. 29 ds. ochrony danych, przyjęła w dniu 16 lutego 2010 r. Dokument Roboczy w sprawie pojęć „administrator danych” i „przetwarzający” (WP 169). Zgodnie z treścią ww. opinii określenie „celu” przetwarzania danych jest zastrzeżone dla „administratora danych”. Ktokolwiek podejmuje tę decyzję jest faktycznie administratorem danych. Administrator danych może przekazać określenie „sposobów” przetwarzania w odniesieniu do kwestii technicznych i organizacyjnych. Zasadnicze kwestie dotyczące zgodności przetwarzania danych z prawem należą do administratora danych. Osoba

---

<sup>199</sup> DOLIS-035-873/12/ 22694

lub podmiot, które podejmują decyzję dotyczącą np. tego, jak długo przechowuje się dane lub kto ma do nich dostęp, działają jako „administrator danych” w odniesieniu do tej części wykorzystywania danych, a zatem muszą spełniać wszystkie obowiązki administratora danych. Generalny Inspektor zaznaczył również, iż „brak możliwości bezpośredniego wywiązania się ze wszystkich obowiązków administratora danych (zapewnienie informacji, prawa dostępu, itp.) nie wyklucza możliwości bycia administratorem. Może zdarzyć się, że w praktyce obowiązki te mogłyby być z łatwością pełnione w imieniu administratora danych przez inne strony. Administrator danych pozostaje jednak zawsze ostatecznie odpowiedzialny za swoje obowiązki i będzie odpowiadał za ich niewypełnienie. Odnosząc się zaś do pojęcia „przetwarzającego dane” Grupa Robota Art. 29 ds. ochrony danych osobowych wskazała m.in., że *„rola przetwarzającego nie wynika z charakteru osoby prawnej przetwarzającej dane, ale z jej konkretnej działalności w określonym kontekście. Innymi słowy, ta sama osoba prawna może działać jednocześnie jako administrator danych w przypadku niektórych operacji przetwarzania danych oraz jako przetwarzający w przypadku innych tego rodzaju operacji, a kwalifikowanie się jako administrator danych lub przetwarzający należy oceniać w odniesieniu do określonych zestawów danych lub operacji.”* W tym miejscu Generalny Inspektor przyznał, że pomocne tu mogą być orzeczenia Naczelnego Sądu Administracyjnego zapadłe w indywidualnych sprawach, które będzie można odnieść do niniejszej analizy kwestii, któremu z podmiotów przysługuje status administratora danych - czy instytucji zarządzającej, czy może instytucji wdrażającej program finansowany ze środków UE. Generalny Inspektor wskazał, że nie oznacza to, iż w innych sprawach dotyczących tej materii zapadłyby podobne orzeczenia. Zarówno orzeczenia sądów administracyjnych, jak i decyzje Generalnego Inspektora Ochrony Danych Osobowych wydawane są w oparciu o konkretny stan faktyczny. Konkludując, nie można w sposób jednoznaczny, na potrzeby wszelkich programów operacyjnych realizowanych obecnie w Polsce uznać, że zawsze, w każdym przypadku administratorem danych przetwarzanych w związku z finansowaniem działań ze środków z UE będzie Polska Agencja Rozwoju Przedsiębiorczości, czy też Minister Rozwoju Regionalnego. Mogą zdarzyć się bowiem sytuacje, gdy w jednym, z programów operacyjnych podmiotem decydującym o celach i środkach przetwarzania danych określonych osób będzie Polska Agencja Rozwoju Przedsiębiorczości, w innym zaś Minister Rozwoju Regionalnego. Zaznaczyć należy, że status administratora danych może zostać przypisany danemu podmiotowi jedynie w oparciu o analizę wszelkich okoliczności faktycznych i prawnych unormowań występujących w procesie przetwarzania danych, a nie zaś o analizę formalną.

Kolejnym wartym przedstawienia w niniejszym *Sprawozdaniu* zagadnieniem była nadesłana w dniu 22 października 2012 r. z Helsińskiej Fundacji Praw Człowieka prośba o skierowanie wystąpienia do Ministra Sprawiedliwości w przedmiocie zmian prawnych dotyczących niektórych kwestii związanych z **jawnością wokand sądowych w sądownictwie powszechnym**. W odpowiedzi

GIODO poinformował,<sup>200</sup> że sprawa przetwarzania danych osobowych w treści wokand jest Generalnemu Inspektorowi Ochrony Danych Osobowych znana. Polski organ ochrony danych osobowych pozostaje orędownikiem zmiany aktualnie obowiązującego stanu prawnego tak, ażeby ewentualne prawo do zamieszczania określonego (ograniczonego w pewnych sytuacjach – w zależności od kategorii spraw) zakresu danych osobowych nie wynikało z przepisów o charakterze wewnętrznym (w tym konkretnym przypadku z treści zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej – Dz. Urz. MS Nr 5, poz. 22 z późn. zm.), a z aktów prawa powszechnie obowiązującego. Generalny Inspektor poinformował, że pozytywnie zaopiniował przesłany przez Ministra Sprawiedliwości *projekt rozporządzenia Ministra Sprawiedliwości zmieniającego rozporządzenie – Regulamin urzędowania sądów powszechnych*, który przewidywał dodanie po art. 67 rozporządzenia Ministra Sprawiedliwości z dnia 23 lutego 2007 r. Regulamin urzędowania sądów powszechnych (Dz. U. Nr 38, poz. 249 z późn. zm.) art. 67a. Projektowany przepis wskazywał m.in., iż w sprawach z zakresu prawa rodzinnego i opiekuńczego nie podaje się przedmiotu sprawy, tylko określa się je jako sprawy z zakresu prawa rodzinnego lub opiekuńczego. Pomimo iż prace nad ww. projektem zostały wstrzymane, to jednakże ze znajdujących się w posiadaniu Generalnego Inspektora informacji wynika, iż Minister Sprawiedliwości rozważa przygotowanie nowego rozporządzenia w tej materii, bądź dokonanie szerokiej nowelizacji aktualnie obowiązującego. Działania te spotkały się z aprobatą Generalnego Inspektora Ochrony Danych Osobowych i są przez niego w pełni popierane. Jednocześnie przypomniał, że wszelkie działania w tej sprawie podejmowane zarówno przez Radę Ministrów, jak i przez Generalnego Inspektora Ochrony Danych Osobowych, nie mogą sprzeciwiać się innej zasadzie leżącej u podstaw działań władzy sądowej w demokratycznym państwie prawnym, jaką jest zasada jawności postępowania sądowego, będąca gwarancją bezstronności i niezależności sędziego. Generalny Inspektor stoi wszakże na stanowisku, że ta podniesiona do rangi konstytucyjnej zasada (art. 45 Konstytucji Rzeczypospolitej Polskiej) nie może być stosowana bez ograniczeń, w sposób naruszający inne konstytucyjne prawa i wolności jednostki, jak np. prawo do prywatności (art. 47 ustawy zasadniczej), czy prawo do ochrony danych osobowych (art. 51). Zaznaczył też, iż istnieje wyraźna różnica pomiędzy jawnością treści zawierających dane osobowe, zamieszczonych w wokandach sądowych a ich powszechną dostępnością czy możliwością ponownego przetwarzania. Dlatego też praktyką niezgodną z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych byłoby zamieszczanie wokand sądowych w sieci Internet i umożliwienie dostępu do danych w niej zawartych niezliczonej grupie osób. Uwzględniając doniosłość zasygnalizowanego problemu Generalny Inspektor Ochrony Danych Osobowych zadeklarował pełną gotowość do

---

<sup>200</sup> DOLiS-035-3165/12/68776

uczestnictwa w ewentualnych pracach zmierzających do prawidłowego uregulowania kwestii przetwarzania danych osobowych w treści wokand sądowych.

Niektóre zapytania kierowane do Generalnego Inspektora Ochrony Danych Osobowych wskazują, że w praktyce - w kontekście określonej sytuacji – w dalszym ciągu wątpliwości budziła **definicja „przetwarzania danych”**. W szczególności chodziło o zagadnienie, czy za „przetwarzanie” należy uznać działanie polegające na dokonywaniu sprawdzeń w określonej bazie informatycznej<sup>201</sup>. W odniesieniu do tego problemu Generalny Inspektor zaznaczył, że zawarta w art. 7 pkt 2 ustawy o ochronie danych osobowych definicja przetwarzania danych jest zakreślona szeroko i obejmuje wszelkiego rodzaju działania na danych, nawet niewymienione w tym przepisie. O przetwarzaniu danych można mówić począwszy od zbierania danych, a skończywszy na ich usunięciu. Generalny Inspektor podniósł, że w komentarzach do tego przepisu wskazuje się, „(...) iż *samo czytanie danych osobowych przez administratora danych lub jego pracownika stanowi już przetwarzanie danych w rozumieniu ustawy. (...) Zwrócił ponadto uwagę, że z materiałów dotyczących prac nad dyrektywą 95/46/WE, w której zamieszczono podobnie szeroką definicję pojęcia przetwarzania danych (processing of personal data), można wnioskować, iż pojęciem przetwarzania zamierzano objąć też operacje wewnątrz przedsiębiorstwa czy innej jednostki organizacyjnej, w której działa administrator, a więc np. przekazywanie danych innym pracownikom jednostki. Za udostępnianie danych należy w każdym razie uznać ich przekazanie innym przedsiębiorstwom należącym do koncernu czy holdingu*”<sup>202</sup>. Jak stwierdził Wojewódzki Sąd Administracyjny w Warszawie w wyroku II SA/Wa 887/04 z dnia 17 listopada 2004 r. przetwarzanie danych nie jest czynnością prawną, lecz czynnością faktyczną, z której wypływają konsekwencje prawne (LEX nr 164505). W doktrynie prawa administracyjnego tego typu działania określa się mianem czynności materialno-technicznych. Generalny Inspektor wskazał też, że potwierdzeniem słuszności szerokiego ujmowania pojęcia „przetwarzania” danych jest również definicja zawarta w projekcie ogólnego rozporządzenia o ochronie danych, zgodnie z którą „przetwarzanie” oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, pobieranie, uzyskiwanie wglądu, wykorzystywanie, ujawnianie poprzez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, dopasowywanie lub łączenie, usuwanie lub niszczenie. Zastrzegł, że ocena wypełnienia przez zachowanie określonej osoby znamion przestępstwa, w konkretnym przypadku nie należy do Generalnego Inspektora Ochrony Danych Osobowych. Niemniej mając na uwadze sposób sformułowania legalnej definicji „przetwarzania danych” oraz dotyczące tego pojęcia stanowisko doktryny stwierdził, że pojęcie to

---

<sup>201</sup> DOLiS-035-2556/12/ 53980

<sup>202</sup> Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Ochrona danych osobowych, Komentarz, Lex, Kraków 2007.

należy rozumieć szeroko i obejmować nim wszelkie działania wykonywane na danych osobowych. Podkreślił też, że z punktu widzenia respektowania zasad ochrony danych osobowych istotne jest, aby dla każdego posłużenia się danymi osobowymi istniała określona podstawa prawna (przesłanka legalności). Podsumowując Generalny Inspektor poinformował, że w każdym przypadku korzystanie z danych (wykonywanie na nich określonych operacji/sprawdzeń) powinno następować jedynie w ścisłym w związku z realizowaniem określonych zadań i uprawnień. Wymóg ten odnosi się niewątpliwie również do przetwarzania danych wewnątrz przedsiębiorstwa/jednostki organizacyjnej przez zatrudnionych w niej pracowników/funkcjonariuszy.

Do Generalnego Inspektora Ochrony Danych Osobowych wpłynęła również prośba o informację w związku z problemem **przekazywania danych osobowych obywateli polskich gromadzonych w Centralnej Ewidencji Pojazdów i Kierowców niemieckim instytucjom**. W odpowiedzi<sup>203</sup> Generalny Inspektor poinformował, że ustawa o ochronie danych osobowych stosuje się do: 1) podmiotów niepublicznych realizujących zadania publiczne, 2) osób fizycznych i osób prawnych oraz jednostek organizacyjnych nie będących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych - które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej. Powołał również art. 7 pkt 7 ustawy o ochronie danych osobowych, zgodnie z którym przez państwo trzecie rozumie się państwo nienależące do Europejskiego Obszaru Gospodarczego. Oznacza to m.in., iż określone ustawą warunki przekazywania danych do państwa trzeciego nie znajdują zastosowania wobec przekazywania danych osobowych do państwa członkowskiego Unii Europejskiej. W tym zakresie, jakiegokolwiek organy kraju członkowskiego UE - co do zasady - są traktowane jak podmioty polskie. Generalny Inspektor wskazał, że ustawa o ochronie danych osobowych, określa zasady postępowania przy przetwarzaniu danych, ujmując je w formę podstawowych obowiązków administratora danych - określa ogólne zasady przetwarzania i ochrony danych osobowych, zaś skonkretyzowanie tychże zasad ma miejsce w szczególnych wobec jej regulacji przepisach prawa. Dlatego, jeżeli istnieją szczególne przepisy prawa regulujące przetwarzanie danych osobowych (w tym udostępnianie, czy pozyskiwanie), to stosuje się je w pierwszej kolejności. Ponadto przypomniał, że zgodnie z art. 5 ustawy o ochronie danych osobowych, jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw. Wskazał, że podmioty publiczne działają na podstawie przepisów prawa, w ramach kompetencji nadanych im tymi przepisami. Zgodnie z przepisami ustawy o ochronie danych osobowych istotne jest, aby administrator danych legitymował

---

<sup>203</sup> DOLiS-035-3143/12



się jedną z przesłanek legalności przetwarzania, w tym udostępnienia danych osobowych, które dla danych tzw. zwykłych (jak np. imię, nazwisko, adres zamieszkania) określone zostały w art. 23 ust. 1 pkt 1-5, zaś katalog danych tzw. szczególnie chronionych zawiera art. 27 ust. 1 – w art. 27 ust. 2 pkt 1-10 ustawy. Dla podmiotów publicznych istotne są te, określone w art. 23 ust. 1 pkt 2 i art. 27 ust. 2 pkt 2 ustawy. Generalny Inspektor podkreślił też, że jedną z przesłanek dopuszczalności przetwarzania danych, określoną w art. 23 ust. 1 pkt 2 ustawy, jest m.in. niezbędność przetwarzania dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W przedmiotowej sprawie dotyczącej udostępnienia danych osobowych obywateli polskich zgromadzonych w Centralnej Ewidencji Pojazdów i Kierowców, zastosowanie mają przepisy ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. 2005 r. Nr 108, poz. 908 z późn. zm.). Jak uznał Generalny Inspektor, ustawa ta stanowi o zasadach udostępnienia danych w zarówno z Centralnej Ewidencji Pojazdów (w Dziale III, Rozdziale 2a tej ustawy) jak i Centralnej Ewidencji Kierowców (w Dziale IV, Rozdziale 1a). Zgodnie z artykułem 80c ust. 1 powyższego aktu prawnego, dane lub informacje zgromadzone w Centralnej Ewidencji Pojazdów udostępnia się, o ile są one niezbędne do realizacji ustawowych zadań określonych w tym przepisie katalogowi podmiotów (z zastrzeżeniem ust. 2). Ponadto zgodnie z ust. 4 ww. artykułu, minister właściwy do spraw wewnętrznych może udostępnić dane lub informacje zgromadzone w ewidencji innym podmiotom (niż wymienione w ust. 1-3), w tym osobom fizycznym, osobom prawnym lub jednostkom organizacyjnym nieposiadającym osobowości prawnej, jeżeli wykażą swój uzasadniony interes. Z kolei art. 80c w ust. 6a stanowi, iż dane lub informacje zgromadzone w ewidencji mogą być udostępniane podmiotom zagranicznym w celu wypełnienia postanowień ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych, a także wykonania aktu prawa stanowionego przez organizację międzynarodową, której Rzeczpospolita Polska jest członkiem. Tryb i sposób udostępniania danych określają ratyfikowane przez Rzeczpospolitą Polską umowy międzynarodowe, akty prawa stanowionego przez organizację międzynarodową, której Rzeczpospolita Polska jest członkiem lub porozumienia zawarte pomiędzy właściwymi ministrami państw członkowskich Unii Europejskiej. Generalny Inspektor wskazał również, że odnośnie Centralnej Ewidencji Kierowców o przedmiotowych kwestiach stanowi art. 100c ustawy Prawo o ruchu drogowym, w szczególności ust. 1 (zawierający katalog podmiotów, którym dane mogą być udostępniane), ust. 4 (traktujący o wnioskowym trybie udostępniania danych) i ust. 4a - o uprawnieniu do udostępnienia danych podmiotom zagranicznym w celu wypełnienia postanowień ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych, a także wykonania aktu prawa stanowionego przez organizację międzynarodową, której Rzeczpospolita Polska jest członkiem. Wspomniał również o Konwencji o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej, sporządzonej w Brukseli dnia 29 maja 2000 r. (Dz.U. 2007 r. Nr 135, poz. 950), czy 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.U.U.E.L.2008.350.60). Podkreślił jednak, iż ocena legalności przetwarzania – w tym udostępnienia - danych osobowych osoby fizycznej, zawsze powinna następować w odniesieniu do skonkretyzowanych okoliczności. Zgodnie ze statutem Centralnego Ośrodka Informatyki - stanowiącym załącznik do zarządzenia Nr 48 Ministra Spraw Wewnętrznych i Administracji z dnia 26 listopada 2010 w sprawie utworzenia i nadania statutu instytucji gospodarki budżetowej pod nazwą „Centralny Ośrodek Informatyki” (Dz.Urz.MSW.2010.15.74) – wydanego na podstawie art. 23 ust. 2 pkt 1 i art. 26 ust. 1 i 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. Nr 157, poz. 1240 z późn. zm.), Centralny Ośrodek jest instytucją gospodarki budżetowej, którego przedmiotem podstawowej działalności jest m.in. wykonywanie czynności materialno-technicznych związanych z udostępnieniem danych z Centralnej Ewidencji Pojazdów oraz Centralnej Ewidencji Kierowców.

Interesujące było również pytanie dotyczące **możliwości pozyskiwania informacji na temat nałogu i uczestnictwa w procesie leczenia osób korzystających z pomocy Zespołów Interdyscyplinarnych**. Na wstępie Generalny Inspektor zwrócił uwagę na legalność przetwarzania danych osobowych szczególnie chronionych, uregulowaną w art. 27 ust. 2 pkt 1-10 ustawy o ochronie danych osobowych<sup>204</sup>. Podkreślił, że na mocy art. 27 ust. 2 pkt 2, przetwarzanie danych, o których mowa w ust. 1, jest dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. Działalność zespołów interdyscyplinarnych regulują przepisy 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.). Na mocy art. 6 ust. 1 ww. aktu prawnego, zadania w zakresie przeciwdziałania przemocy w rodzinie są realizowane przez organy administracji rządowej i jednostki samorządu terytorialnego na zasadach określonych w przepisach ustawy z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2009 r. Nr 175, poz. 1362 z późn. zm.) lub ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2007 r. Nr 70, poz. 473 z późn. zm.), chyba że przepisy niniejszej ustawy stanowią inaczej. Powołał treść art. 6 ust. 2 pkt 4 ustawy o przeciwdziałaniu przemocy w rodzinie, zgodnie z którym do zadań własnych gminy należy w szczególności tworzenie gminnego systemu przeciwdziałania przemocy w rodzinie, w tym tworzenie zespołów interdyscyplinarnych. Powołał również art. 50 ust.1 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (t. j. Dz. U. z 2011 r. Nr 231 poz. 1375 z późn. zm.), na mocy którego osoby wykonujące czynności wynikające z niniejszej ustawy są obowiązane do zachowania w tajemnicy wszystkiego, o czym powezmą wiadomość w związku z wykonywaniem tych czynności, stosownie do odrębnych przepisów, a nadto z zachowaniem przepisów niniejszego rozdziału. Przypomniał również

---

<sup>204</sup> DOLiS-035-1444/50561/12

art. 50 ust. 2 i 3, na mocy którego, od obowiązku zachowania tajemnicy osoba wymieniona w ust. 1 jest zwolniona w stosunku do właściwych organów administracji rządowej lub samorządowej co do okoliczności, których ujawnienie jest niezbędne do wykonywania zadań z zakresu pomocy społecznej oraz osób współuczestniczących w wykonywaniu czynności w ramach pomocy społecznej w zakresie, w jakim to jest niezbędne. Zgodnie zaś z art. 14 ust. 1 ustawy z dnia 8 czerwca 2008 r. o zawodzie psychologa i samorządzie zawodowym psychologów (t. j. Dz. U. z 2001 r. Nr 73 poz. 763 z późn. zm.), psycholog ma obowiązek zachowania w tajemnicy informacji związanych z klientem, uzyskanych w związku z wykonywaniem zawodu. Niemniej jednak na mocy ust. 2 ww. przepisu, przepisu ust. 1 nie stosuje się, gdy poważnie jest zagrożone zdrowie, życie klienta lub innych osób albo gdy tak stanowią ustawy. Zwrócił też uwagę na treść art. 9 c ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie, zgodnie z którym członkowie zespołu interdyscyplinarnego oraz grup roboczych w zakresie niezbędnym do realizacji zadań, o których mowa w art. 9b ust. 2 i 3, mogą przetwarzać dane osób dotkniętych przemocą w rodzinie i osób stosujących przemoc w rodzinie, dotyczące: stanu zdrowia, nałogów, skazań, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, bez zgody i wiedzy osób, których dane te dotyczą. Zaznaczył, że art. 9c w swojej dalszej części nakłada na członków przedmiotowych zespołów oraz grup obowiązek zachowania w poufności odnośnie wszelkich informacji oraz danych pozyskanych w ramach ich działania. Jeśli zatem członkowie zespołu interdyscyplinarnego w związku z koniecznością wykonania obowiązków nałożonych na nich przez ustawę o przeciwdziałaniu przemocy w rodzinie przetwarzają dane osobowe o charakterze szczególnie chronionym osób wymagających pomocy, to nie naruszają takim działaniem regulacji określonych w ustawie o ochronie danych osobowych. Wykonują bowiem postanowienia określone przepisami ustawy. Podkreślił jednak, że przetwarzanie takich danych powinno następować w sytuacji, gdy jest to niezbędne do udzielenia pomocy określonym osobom i następować powinno w sposób adekwatny do celu przetwarzania. Zgodnie bowiem z art. 26 ust. 1 pkt 2 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.

Wartym wskazania w przedmiotowym *Sprawozdaniu* było pytanie skierowane z Ministerstwa Pracy i Polityki Społecznej **w sprawie obowiązków wynikających z ustawy o ochronie danych osobowych w związku z prowadzeniem jawnego rejestru agencji zatrudnienia**. Generalny Inspektor poinformował<sup>205</sup>, że z dniem 31 grudnia 2011 r. stracił moc obowiązującą art. 7a ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej (Dz. U. Nr 101, poz. 1178 z późn. zm.), który stanowił, że ewidencja działalności gospodarczej jest jawna i dane osobowe w niej

---

<sup>205</sup> DOLIS -035-523/12/14892

zawarte nie podlegają przepisom ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Generalny Inspektor wskazał, iż w konsekwencji od 1 stycznia 2012 r. przepisy ww. ustawy, dotyczą już informacji identyfikujących przedsiębiorców w obrocie gospodarczym, o ile – dla konkretnego stanu faktycznego – będą stanowiły dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych. Tym samym administratorzy danych osobowych dotyczących przedsiębiorców muszą wypełniać wszelkie obowiązki wynikające z ustawy o ochronie danych osobowych, w tym te dotyczące legalności przetwarzania danych osobowych, z uwzględnieniem wyjątków stanowiących przepisami prawa, w tym ustawy o ochronie danych osobowych. Generalny Inspektor przytoczył definicję administratora danych i zaznaczył, że w przypadku podmiotów publicznych mogą one decydować o celu przetwarzania danych osobowych w ramach zadań, jakie wykonują zgodnie z przepisami prawa, i które tymi przepisami zostały wyznaczone. Innymi słowy, rozstrzygnięcie, któremu podmiotowi działającemu w sektorze publicznym przysługuje status administratora danych, wymaga analizy przepisów prawa w oparciu, o które podmiot ten działa. Stosownie do art. 40 ustawy o ochronie danych osobowych, obowiązek zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 pkt 1-11<sup>206</sup> ustawy, spoczywa na administratorze danych. Generalny Inspektor podkreślił, że wyjątków tych nie można interpretować rozszerzająco. W każdym przypadku przetwarzania danych osobowych, to ich administrator powinien dokonać oceny, czy ze względu na charakter przetwarzanych danych ich zbiór podlega obowiązkowi zgłoszenia do rejestracji. Zwolnienie zbioru z rejestracji jest możliwe tylko wówczas, gdy opisana w art. 43 ust. 1 ustawy przesłanka dotyczy wszystkich danych zawartych w tym zbiorze. Jeśli więc w ramach tworzonych zbiorów przetwarzane są, choćby incydentalnie, dane inne, niż te wymienione w art. 43 ust. 1 bądź w innym celu niż wskazane w tym przepisie, to zbiór podlega wówczas obowiązkowi zgłoszenia do rejestracji. Generalny Inspektor przytoczył brzmienie art. 43 ust.

---

<sup>206</sup> Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych: 1)<sup>(53)</sup> 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)<sup>(54)</sup> przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, 2c)<sup>(55)</sup> przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, 3)<sup>(56)</sup> dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego, 4)<sup>(57)</sup> 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, rzeczownika patentowego, doradcy podatkowego lub biegłego rewidenta, 6)<sup>(58)</sup> 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.

1 pkt 9 ustawy o ochronie danych osobowych, i zaznaczył, że przesłanka ta jest spełniona, jeżeli z danymi zawartymi w administrowanym zbiorze może zapoznać się bez szczególnego nakładu sił i środków nieograniczony krąg podmiotów. Powszechnie dostępne muszą być wszystkie, a nie tylko niektóre dane zawarte w zbiorze danych. O ile zbiór danych spełni wskazane powyżej warunki, tj. powszechna dostępność wszystkich danych gromadzonych w nim, to taki zbiór może wypełniać przesłankę zbioru danych powszechnie dostępnych, który nie podlega obowiązkowi zgłoszenia do rejestracji. Jednocześnie Generalny Inspektor dodał, że z powyższego zwolnienia z rejestracji mogą korzystać jedynie zbiory, których celem przy ich tworzeniu była jawność, co wynika z przepisów szczególnych. W przypadku zaś, gdy zbiór danych powstaje na nowo, lecz ze źródeł powszechnie dostępnych, a normy prawne regulujące kwestie związane ze sposobem jego działania nie przewidują powszechnej dostępności całego zbioru, wówczas zbiór taki podlega rejestracji. W tym miejscu wskazać należy przepisy ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (t. j. Dz. U. z 2008 r. Nr 69, poz. 415 z późn. zm.), w szczególności jej art. 18d, który stanowi, iż rejestr prowadzi marszałek województwa właściwy dla siedziby podmiotu ubiegającego się o wpis. Rejestr jest jawny i może być prowadzony w formie dokumentu elektronicznego (ust. 2 ww. przepisu). Zgodnie zaś z art. 18r cytowanej ustawy, minister właściwy do spraw pracy przetwarza dane o agencjach zatrudnienia przekazane w formie dokumentu elektronicznego przez marszałków województw. Generalny Inspektor podsumował, że w opisanej sprawie, niewątpliwie przepisy ustawy o promocji zatrudnienia i instytucjach rynku pracy wskazują, jakie podmioty tworzą zbiory agencji zatrudnienia, określając ich obowiązki w tym zakresie, a także nadając im szczególne uprawnienia i decyzyjność w poszczególnych obszarach oraz stanowią, które zbiory są jawne. Nadmieniał również, że wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych 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). Ponadto podkreślił, że jeśli administrator danych zgłosi zbiór danych do rejestracji mimo braku takiego obowiązku, to Generalny Inspektor na podstawie art. 105 § 1 K.p.a. po stwierdzeniu bezprzedmiotowości postępowania, wydaje decyzję o umorzeniu takiego postępowania rejestracyjnego.

W analizowanym 2012 roku Generalny Inspektor skierował również sygnalizację do organu samorządu terytorialnego **w sprawie załączania do pism z prowadzonego przez ten organ postępowania administracyjnego, wykazu zawierającego dane osobowe stron postępowania**<sup>207</sup>. Generalny Inspektor zwrócił się o zmianę stosowanej praktyki w celu zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa. Wskazał, iż administrator

---

<sup>207</sup> DOLiS-035-2623/12

danych osobowych, tj. podmiot decydujący o celach i środkach przetwarzania danych osobowych, obowiązany jest respektować w procesie przetwarzania danych osobowych wszelkie zasady wynikające z przepisów o ochronie danych osobowych. Podkreślił też, że z punktu widzenia przepisów o ochronie danych osobowych istotne jest przede wszystkim, aby czynność przetwarzania danych osobowych przez administratora danych, znajdowała podstawę w jednej z ustawowych przesłanek legalizacyjnych określonych w art. 23 ust 1 pkt 1-5 ustawy. Spełnienie jednego z warunków wskazanych w powołanym przepisie stanowi o zgodnym z prawem przetwarzaniu danych osobowych, gdyż przesłanki te są równoprawne, a jednocześnie autonomiczne. Generalny Inspektor podniósł zatem, że przetwarzanie danych osobowych może być uznane za legalne m.in. wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych (art. 23 ust. 1 pkt 1 ustawy), lub gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy). W dalszej części sygnalizacji Generalny Inspektor powołał treść art. 107 § 1 ustawy z dnia 14 czerwca 1970 r. Kodeks postępowania administracyjnego (t. j. Dz. U. z 2000 r. Nr 98 poz. 1071 z późn. zm.)<sup>208</sup> wskazując, że stanowi on podstawę do określenia w treści decyzji strony/stron postępowania oraz konieczność stwierdzenia, że rozstrzygnięcie zostało wydane w stosunku do konkretnej strony. Przypomniał także stanowisko Wojewódzkiego Sądu Administracyjnego, który w wyroku z dnia 20 października 2005 roku wydanym w sprawie o sygnaturze akt III SA/Wa 1517/2005, stwierdzając, iż: „(...) Adresat decyzji powinien być oznaczony wprost... Wątpliwości co do adresata zaskarżonej decyzji nie może usunąć, zamieszczony pod tą decyzją tzw. „rozdzielnik”, tzn. wykaz podmiotów, które decyzję otrzymują. Z całą mocą zaznaczyć należy, iż adresat decyzji nie może być oznaczony w sposób dorozumiany i miejscem jego oznaczenia nie może być to, w którym wskazuje się osoby, które decyzję otrzymują, czy też poprzez wskazanie osoby, która wniosła odwołanie. (...)”. Generalny Inspektor przyznał, że wprowadzie przepisy K.p.a. przewidują dopuszczalność zapoznania się przez stronę w toku postępowania administracyjnego z danymi innych uczestników postępowania oraz nakładają na organ administracji obowiązek należytego i wyczerpującego informowania stron o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie ich praw i obowiązków będących przedmiotem postępowania, jednakże nie statuują wprost wymogu umieszczania w korespondencji kierowanej do stron postępowania wykazu (rozdzielnika) zawierającego dane pozostałych jego uczestników. W opinii Generalnego Inspektora Ochrony Danych Osobowych osiągnięcie efektu zapewnienia stronom postępowania realizacji przysługujących im uprawnień (prawa do informacji na temat toczącego się

---

<sup>208</sup> Decyzja powinna zawierać: oznaczenie organu administracji publicznej, datę wydania, oznaczenie strony lub stron, powołanie podstawy prawnej, rozstrzygnięcie, uzasadnienie faktyczne i prawne, pouczenie, czy i w jakim trybie służy od niej odwołanie, podpis z podaniem imienia i nazwiska oraz stanowiska służbowego osoby upoważnionej do wydania decyzji. Decyzja, w stosunku do której może być wniesione powództwo do sądu powszechnego lub skarga do sądu administracyjnego, powinna zawierać ponadto pouczenie o dopuszczalności wniesienia powództwa lub skargi.

postępowania) jest możliwe w inny sposób, np. poprzez wysłanie pism (zawiadomień, postanowień, decyzji) bez załączania rozdzielnika zawierającego dane wszystkich uczestników, który to wykaz jest ważny przede wszystkim dla organu prowadzącego postępowanie. W przypadku wysyłania pism o zbiorczym charakterze wydaje się zasadne, aby dane osobowe wszystkich adresatów zamieszczane były na odrębnej karcie (rozdzielniku), pozostającej jedynie w dyspozycji organu, a pisma rozsyłane były następnie indywidualnie do każdego z zainteresowanych uczestników, bez przesyłania każdemu z nich listy imion, nazwisk i adresów pozostałych osób. Wykaz adresatów pozostawać wówczas powinien w aktach sprawy. W świetle powyższego Generalny Inspektor zaznaczył, że strony w toczącym się postępowaniu administracyjnym były uprawnione do zapoznawania się z informacjami zawartymi w materiale zgromadzonym w tym postępowaniu, w tym z danymi osobowymi identyfikującymi pozostałe strony. W ocenie Generalnego Inspektora Ochrony Danych Osobowych zbędne było przesyłanie stronom postępowania pełnego rozdzielnika do pism urzędowych, zawierającego ich imiona, nazwiska i adresy zamieszkania.

#### 7.1.4. 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 2012 roku Generalny Inspektor Ochrony Danych Osobowych skierował **126** takich wystąpień i sygnalizacji.

Poniżej przedstawione zostały przykłady 11 wystąpień Generalnego Inspektora skierowanych **do podmiotów administracji publicznej** w celu dostosowania obecnie obowiązujących przepisów prawa do zasad prawidłowego przetwarzania danych osobowych.

Wśród nich znalazło się wystąpienie z dnia 13 lutego 2012 r.<sup>209</sup> skierowane do Minister Edukacji Narodowej, w którym Generalny Inspektor Ochrony Danych Osobowych zasygnalizował potrzebę podjęcia prac legislacyjnych mających na celu przeniesienie regulacji zawartych w rozporządzeniu Ministra Edukacji Narodowej z dnia 27 października 2009 r. w sprawie wymagań, jakim powinna odpowiadać osoba zajmująca stanowisko dyrektora oraz inne stanowisko kierownicze w poszczególnych typach publicznych szkół i rodzajach publicznych placówek (Dz. U. z 2009 r. Nr 184, poz. 1436) do aktu prawnego rangi ustawowej. Wskazał przy tym, że na kanwie opiniowania projektu rozporządzenia Ministra Kultury i Dziedzictwa Narodowego zmieniającego rozporządzenie w sprawie regulaminu konkursu na stanowisko dyrektora szkoły lub placówki oraz trybu pracy komisji konkursowej<sup>210</sup>, ujawnił się problem związany z uprawnieniem wynikającym z przepisów tego rozporządzenia, do pozyskiwania od kandydatów na dyrektorów takich danych, jak np. dane o karalności za przestępstwa ścigane z oskarżenia publicznego. W świetle powyższego Generalny Inspektor powołał art. 47<sup>211</sup> oraz 51<sup>212</sup> Konstytucji Rzeczypospolitej Polskiej podkreślając, że ograniczenia w zakresie korzystania z prawa do ochrony życia prywatnego i decydowania o swoim życiu osobistym wymagają bezwzględnie regulacji rangi ustawowej (art. 31 ust. 3 Konstytucji RP). Przypomniawszy też cytowane wcześniej postanowienie Trybunału Konstytucyjnego z dnia 31 stycznia 2007 roku (sygn. akt S 1/2007) o zasadzie wyłączności regulacji ustawowej w sferze praw i wolności oraz niedopuszczalności cedowania przez Parlament funkcji prawodawczych na organy władzy wykonawczej. Ponadto Generalny Inspektor powołał art. 31<sup>213</sup> Konstytucji RP, który statuuje tzw. zasadę proporcjonalności. Zdaniem Generalnego Inspektora, godząc się na limitowanie konstytucyjnych praw i wolności, ustawodawca precyzuje warunki dopuszczalności tego rodzaju ograniczeń. Dodał również, że Trybunał Konstytucyjny w swym orzecznictwie wielokrotnie wskazywał, że art. 31 ust. 3 Konstytucji RP precyzyjnie określa przesłanki dopuszczalności ograniczeń w korzystaniu z wolności i praw jednostki. Należą do nich: a) ustawowa forma ograniczeń, b) funkcjonalny związek ograniczenia z realizacją wartości wskazanych

---

<sup>209</sup> DOLiS-035-453/12/KS/10419

<sup>210</sup> Znowelizowane rozporządzenie zostało wydane na podstawie art. 36a ust. 12 ustawy z dnia 7 września 1991 r. o systemie oświaty, Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.

<sup>211</sup> Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

<sup>212</sup> Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

<sup>213</sup> Wolność człowieka podlega ochronie prawnej. 2. Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje. 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.



enumeratywnie w art. 31 ust. 3 Konstytucji, c) istnienie konieczności ograniczeń, przy braku innych środków skutecznie służących temu celowi, d) zakaz naruszania istoty danej wolności lub prawa<sup>214</sup>. W ocenie Generalnego Inspektora Ochrony Danych Osobowych, oświadczenia uzyskiwane od kandydatów na dyrektorów szkół, iż m.in. nie byli skazani prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe, że nie toczy się przeciwko nim postępowanie karne lub dyscyplinarne, ani też nie byli karani zakazem pełnienia funkcji związanych z dysponowaniem środkami publicznymi danej placówki, stanowią szczególny rodzaj danych osobowych. W ocenie organu oświadczenie o niekaralności również stanowi informację o orzeczeniach wydanych w postępowaniu sądowym. Jak zauważył Generalny Inspektor, ustawodawca - wzorem rozwiązań funkcjonujących w innych państwach oraz postanowień umów międzynarodowych - wyodrębnił pewne kategorie informacji, szczególnie ważnych dla ochrony prywatności każdego człowieka. Inaczej niż w przypadku pozostałych danych osobowych, dane te zostały objęte zakazem przetwarzania, o którym stanowi art. 27 ust. 1<sup>215</sup> ustawy o ochronie danych osobowych. Generalny Inspektor podkreślił, że wyjątki od tego zakazu regulowane są w ust. 2 tegoż artykułu - w szczególności za istotny dla analizowanego stanu faktycznego uznać należałoby art. 27 ust. 2 pkt 2<sup>216</sup> ustawy o ochronie danych osobowych. Generalny Inspektor przyjął, że treść oświadczeń, dotyczących m.in. karalności podlega dyspozycji art. 27 ust. 1 ustawy o ochronie danych osobowych. W tym stanie prawnym, dla tworzenia przepisów aktów prawnych zobowiązujących osoby fizyczne do składania określonych oświadczeń zawierających ich dane osobowe oraz informacje o toczących się przeciwko nim postępowaniach (sądowych lub dyscyplinarnych, zawierających w każdym przypadku dane szczególnie chronione), kluczowym jest istnienie stosownej podstawy prawnej umożliwiającej określonemu podmiotowi uzyskanie kompetencji dla takiego przetwarzania danych osobowych. Zwłaszcza, że w wyniku takiego działania dochodzić miałyby do przetwarzania danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych. W obecnym stanie prawnym wymagania, jakie powinna spełniać osoba kandydująca na stanowisko dyrektora placówki oświatowej, określa ww. rozporządzenie Ministra Edukacji Narodowej z dnia 27 października 2009 r. - a zatem akt wykonawczy. Ponadto regulamin konkursu na stanowisko dyrektora również został określony w akcie prawnym niższym rangą niż ustawa – w rozporządzeniu Ministra Edukacji Narodowej z dnia 8 kwietnia 2010 r. w sprawie regulaminu konkursu na stanowisko dyrektora publicznej szkoły lub publicznej placówki oraz trybu pracy komisji konkursowej (Dz. U. z 2010 r. Nr 60, poz. 373),

---

<sup>214</sup> Wyrok TK z dnia 15 grudnia 2004 r. K. 2/2004 OTK ZU 2004/11A poz. 117; por. też np. wyrok TK z dnia 29 czerwca 2001 r. K. 23/2000 OTK ZU 2001/5 poz. 124, czy wyrok z dnia 12 stycznia 2000 r. P. 11/98 OTK ZU 2000/1 poz. 3.

<sup>215</sup> 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.

<sup>216</sup> Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli przepis szczególnie innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

w przypadku zaś placówek oświatowych - w rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 1 czerwca 2010 r. w sprawie regulaminu konkursu na stanowisko dyrektora szkoły lub placówki oraz trybu pracy komisji konkursowej (Dz. U. z 2010 r. Nr 100, poz. 642). Zdaniem Generalnego Inspektora zasadnym było określenie wymagań, jakim powinny odpowiadać osoby kandydujące na stanowisko dyrektora placówki oświatowej, w przepisach rangi ustawowej, tj. w ustawie z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.). Wówczas istniałaby podstawa do pozyskiwania od kandydatów na stanowisko dyrektora placówki oświatowej takich informacji, jak. m.in. dane o karalności, w akcie prawnym o randze ustawy, a zatem zgodnie z wymogami określonymi w art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych i ustawą zasadniczą. W związku z powyższym Generalny Inspektor wskazał, że ponownej analizy wymaga treść istniejących w tej materii przepisów prawa. Przedmiotowy problem ujawnił się w związku z opiniowaniem przez organ do spraw ochrony danych osobowych projektu rozporządzenia Ministra Kultury i Dziedzictwa Narodowego zmieniającego rozporządzenie w sprawie regulaminu konkursu na stanowisko dyrektora szkoły lub placówki oraz trybu pracy komisji konkursowej. Nie był natomiast wcześniej przedmiotem uwag w trakcie prac legislacyjnych przy zmianach wprowadzanych w rozporządzeniu Ministra Edukacji Narodowej z dnia 27 października 2009 r. w sprawie wymagań, jakim powinna odpowiadać osoba zajmująca stanowisko dyrektora oraz inne stanowisko kierownicze w poszczególnych typach szkół i rodzajach placówek oraz w rozporządzeniu Ministra Edukacji Narodowej z dnia 8 kwietnia 2010 r. w sprawie regulaminu konkursu na stanowisko dyrektora publicznej szkoły lub publicznej placówki oraz trybu pracy komisji konkursowej (Dz. U. z 2010 r. Nr 60, poz. 37). W związku z koniecznością przestrzegania zasad prawidłowej legislacji i poszanowania praw osób, których dane dotyczą (szczególnie w tak newralgicznym obszarze, jakim jest przetwarzanie danych o karalności), Generalny Inspektor uznał, iż niezbędne było przeprowadzenie kompleksowych zmian norm prawnych dotyczących kwestii powierzania stanowiska dyrektora placówki oświatowej, w tym organizowania konkursu na to stanowisko, polegających na umieszczeniu w przepisach rangi ustawowej podstawy prawnej do przetwarzania tej kategorii danych osobowych kandydatów na dyrektorów. W ocenie Generalnego Inspektora, dotychczas przyjęta systematyka, w myśl której w przepisach rozporządzeń daje się uprawnienie do pozyskiwania od kandydatów na dyrektorów placówek oświatowych, danych tzw. szczególnie chronionych (m.in. danych dotyczących orzeczeń wydanych w postępowaniu sądowych lub administracyjnym), pozostaje w sprzeczności z zasadami ochrony danych osobowych.

W odpowiedzi na powyższe wystąpienie, pismem z dnia 27 czerwca 2012 r. (znak: DWST-WPZN-423/115/BSZ/12) Minister Edukacji Narodowej poinformował, że kierowany przez niego resort nie pracuje obecnie nad zmianami przepisów prawa w zakresie statusu dyrektora szkoły. Niemniej jednak zostały zainicjowane rozmowy z przedstawicielami jednostek samorządu terytorialnego

i związków zawodowych na temat zmian w systemie edukacji, w tym również dotyczących statusu dyrektora szkoły i jego pozycji w nowoczesnym systemie edukacji. Minister Edukacji poinformował również, że uwagi Generalnego Inspektora Ochrony Danych Osobowych sformułowane w przedmiotowym wystąpieniu zostaną rozpatrzone w toku prac systemowych nad rozwiązaniami prawnymi dotyczącymi dyrektora szkoły.

Celem wystąpienia skierowanego do **Polskiej Izby Ubezpieczeń w dniu 17 lutego 2012 r.**<sup>217</sup>, było podjęcie stosownych kroków w celu unaocznienia zakładom ubezpieczeń możliwości naruszenia przepisów o ochronie danych osobowych, poprzez **stosowanie praktyki polegającej na dopisywaniu w tytułach przelewów (np. z tytułu świadczenia umowy ubezpieczenia) dodatkowych informacji, w szczególności o charakterze danych szczególnie chronionych, identyfikujących przyczynę wypłaty odszkodowania.** Impulsem do niniejszego wystąpienia było pytanie skierowane do GODO przez ubezpieczonych, którzy otrzymali przelew z tytułu świadczenia umowy ubezpieczenia, zawartej z PZU S.A., opatrzony dopiskiem „Z TYTUŁU URODZENIA MARTWEGO DZIECKA”. Przelew ten został dokonany za pośrednictwem banku PKO BP S.A., któremu informacja o tym tytule została przekazana. Jak zauważył Generalny Inspektor, legalność przetwarzania danych osobowych, w tym ich udostępniania przez administratora danych, uzależniona jest od legitymowania się przez niego jedną z przesłanek wymienionych w art. 23 ust. 1 pkt 1-5 tejże ustawy (w przypadku przetwarzania tzw. danych zwykłych, np. imię, nazwisko, adres, numer telefonu) i/lub w jej art. 27 ust. 2 pkt 1-10 (gdy przetwarzane są tzw. dane szczególnie chronione, których katalog został wskazanych w art. 27 ust. 1). Generalny Inspektor podkreślił, że ustanowione w powołanych przepisach zasady warunkujące zgodne z prawem przetwarzanie danych osobowych, mają charakter równoprawny. Oznacza to, że dla wykazania legalności przetwarzania danych przez określony podmiot wystarcza spełnienie jednej z nich. Jeśli istnieje przesłanka legalizująca udostępnienie danych osobowych, administrator danych, który miałby je przekazać innemu podmiotowi, obowiązany jest również zachować zasady wynikające z art. 26 ust. 1 pkt 1 – 3 ustawy. Generalny Inspektor przypomniał, że 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 przetwarza (np. udostępnia) dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane. Generalny Inspektor wskazał również, że art. 26 ust. 1 pkt 3 ustawy określa w szczególności zakaz zbierania wszelkich danych, niemających znaczenia dla celu, w jakim są zbierane, jak i danych o większym, niż uzasadniony tym celem, stopniu szczegółowości. Pozyskiwanie danych w zakresie szerszym uznane jest za naruszenie zasady adekwatności ustanowionej powołanym przepisem. Zdaniem Generalnego Inspektora przy

---

<sup>217</sup> DOLiS-035-522/12/10581

dokonywaniu wypłat z tytułu świadczenia umowy ubezpieczenia i korzystania z pośrednictwa banku w realizacji tej operacji, nie znajduje uzasadnienia praktyka polegająca na nadawaniu przelewom tytułów o charakterze mogącym naruszyć prywatność osoby fizycznej. Bez wątpienia zakład ubezpieczeń – także dla dokonania stosownego przelewu – dysponuje wystarczającymi informacjami identyfikującymi odbiorcę, osobę uprawnioną, bez konieczności wskazywania dodatkowych informacji identyfikujących przyczynę wypłaty ubezpieczenia. Generalny Inspektor uznał, że wystarczającym identyfikatorem do ustalenia tożsamości strony umowy ubezpieczenia, w relacji tej osoby z zakładem ubezpieczeń – oprócz imienia, nazwiska, adresu zamieszkania – jest np. kod i numer polisy ubezpieczeniowej.

W odpowiedzi na powyższe wystąpienie Polska Izba Ubezpieczeń zobowiązała się podjąć działania mające na celu wyeliminowanie tego rodzaju praktyk w przyszłości.

**Z kolei wystąpienie z dnia 23 marca 2012 r.<sup>218</sup> skierowane do Ministra Transportu, Budownictwa i Gospodarki Morskiej zawierało prośbę o podjęcie prac legislacyjnych w celu zmiany art. 16 ust. 3 ustawy z dnia 15 listopada 1984 r. Prawo przewozowe (Dz. U. z 2000 r. Nr 50, poz. 601 z późn. zm.) dotyczącego zakresu danych osobowych, jaki może być umieszczony na bilecie stanowiącym potwierdzenie zawarcia umowy przewozu.** Na wstępie Generalny Inspektor zacytował art. 16<sup>219</sup> Prawa przewozowego wskazując, że katalog tych informacji - wypracowany praktyką handlową i organizacyjną przewozów - został określony przez ustawodawcę w sposób precyzyjny. Niemniej jednak z punktu widzenia regulacji wynikających z ustawy o ochronie danych osobowych, wątpliwości wzbudzało postanowienie art. 16 ust. 3 ustawy Prawo przewozowe. Informacje, o których stanowi w/w przepis, zapisywane były w pamięci elektronicznej biletu, jeżeli bilet miał formę elektroniczną (art. 16 ust. 4). Generalny Inspektor przywołał tu zasadę adekwatności danych osobowych w stosunku do celów ich przetwarzania. Podniósł również, że ograniczenie dowolności i uznaniowości w tym względzie poprzez precyzyjne określenie zakresu przetwarzanych danych pozwoli uniknąć gromadzenia danych „na zapas”. Generalny Inspektor przypomniał, że zakres danych powinien z jednej strony być wystarczający dla osiągnięcia określonego celu ich przetwarzania, z drugiej zaś, oczywistym jest konieczność takiego jego określenia, aby w żadnym względzie realizacji tego celu nie utrudniał. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych niezbędne było podjęcie prac legislacyjnych zmierzających do doprecyzowania zamkniętego katalogu danych

---

<sup>218</sup> DOLiS-035-880/12/19195

<sup>219</sup> Umowę przewozu zawiera się przez nabycie biletu na przejazd przed rozpoczęciem podróży lub spełnienie innych określonych przez przewoźnika lub organizatora publicznego transportu zbiorowego warunków dostępu do środka transportowego, a w razie ich nieustalenia - przez samo zajęcie miejsca w środku transportowym. Na bilecie, o którym mowa w ust. 1, umieszcza się: 1) nazwę przewoźnika lub organizatora publicznego transportu zbiorowego, 2) relację lub strefę przejazdu, 3) wysokość należności za przejazd, 4) zakres uprawnień pasażera do ulgowego przejazdu. Na bilecie mogą być umieszczane inne informacje, w tym dane osobowe pasażera, jeżeli jest to niezbędne dla przewoźnika lub organizatora w regularnym przewozie osób. Dane i informacje, o których mowa w ust. 2 i 3, zapisywane są w pamięci elektronicznej biletu, jeżeli bilet ma formę elektroniczną.

osobowych pasażera umieszczanych na bilecie, aby były one wystarczające dla udowodnienia prawa do przejazdu. Generalny Inspektor podniósł także, iż określając zakres danych osobowych umieszczony na bilecie przyjąć należy, że powinny to być: imię, nazwisko oraz wizerunek pasażera. W odniesieniu zaś do karty biletu imiennego (karty), który nie miałaby obejmować w swej treści wizerunku jego właściciela, zdaniem Generalnego Inspektora za uzasadnione i adekwatne uznać należałoby zamieszczenie na nim, obok imienia i nazwiska, np. cech dokumentu tożsamości. Ujawnienie innych danych w treści karty/biletu imiennego, np. numeru PESEL, powoduje, iż dostęp do tego rodzaju danych mogłyby mieć osoby nieupoważnione, np. kontrolujący bilety. Tymczasem - jak zauważył Generalny Inspektor - z Prawa przewozowego wynika, że kontrolerzy mogą mieć dostęp do danych tylko w określonych sytuacjach i na podstawie ściśle określonych dokumentów, które świadczą o tożsamości osoby.

W odpowiedzi na stanowisko Generalnego Inspektora, Minister Transportu Budownictwa i Gospodarki Morskiej podzielił uwagi organu do spraw ochrony danych osobowych i wskazał, że problem ten rozwiązany zostanie poprzez nowelizację ustawy Prawo przewozowe.

W wystąpieniu z dnia 23 marca 2012 r.<sup>220</sup> skierowanym do Ministra Pracy i Polityki Społecznej, Generalny Inspektor Ochrony Danych Osobowych wskazał na konieczność podjęcia prac legislacyjnych mających na celu prawne uregulowanie zasad i sposobu prowadzenia dokumentacji przez psychologów. Problem braku szczegółowych regulacji dotyczących zasad i sposobu prowadzenia, w tym udostępniania, dokumentacji związanej ze świadczeniem usług psychologicznych, był niejednokrotnie sygnalizowany organowi ochrony danych osobowych. Przedmiotem zgłaszanych wątpliwości były przede wszystkim zdarzające się w praktyce przypadki odmowy umożliwienia wglądu w dokumentację tworzoną przez psychologów, w tym, np. w wyniki przeprowadzonych badań. Generalny Inspektor zauważył, że regulacje, które odnoszą się do przedmiotowego zagadnienia są bardzo ograniczone, natomiast tryb postępowania, jego przebieg oraz sposób udostępniania wyników tego postępowania, pozostawiony został decyzji psychologa, która następnie powinna być zaakceptowana przez jego klienta. Cytując art. 13 ust. 1<sup>221</sup> ustawy z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów (Dz. U. 73, poz. 763 z późn. zm.) Generalny Inspektor wskazał, iż pozostawienie dowolności w zakresie zasad i sposobu udostępniania informacji/dokumentów dotyczących postępowania z dokumentacją budzi już poważne zastrzeżenia. Ponieważ w obecnym stanie prawnym brak jest przepisów, które regulowałyby zasady i sposób prowadzenia i udostępniania dokumentacji z zakresu psychologii w sposób dostateczny

---

<sup>220</sup> DOLiS-035-893/12/19326

<sup>221</sup> Psycholog poinformuje klienta o celu postępowania, jego przebiegu, wynikach i sposobie ich udostępniania oraz powinien uzyskać akceptację planowanych czynności. Jeżeli wyniki badań mają służyć nie tylko do informacji klienta, stosuje się przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883, z 2000 r. Nr 12, poz. 136, Nr 50, poz. 580 i Nr 116, poz. 1216 oraz z 2001 r. Nr 42, poz. 474 i Nr 49, poz. 509).

i jednoznaczny, w praktyce zdarzały się przypadki odmawiania osobom korzystającym z usług psychologa udostępniania dokumentów zawierających informacje na temat tych osób, z powoływaniem się np. na tajemnicę psychologa lub wskazywaniem, że testy psychologiczne mogą być udostępniane wyłącznie specjalistom. Taka praktyka wzbudziła istotne wątpliwości GODO, ponieważ naruszała przepisy ustawy o ochronie danych osobowych określające katalog praw kontrolnych, przysługujących osobie, której dane dotyczą, tj. art. 32 i następne tej ustawy. Przepisy te zapewniają m.in. uprawnienie do uzyskania informacji dotyczących przetwarzania jej danych osobowych oraz podania ich treści w powszechnie zrozumiałej formie. Na zasadzie analogii należy się również odwołać do przepisów statuujących prawa pacjenta zawarte w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.), w tym w szczególności prawa pacjenta do dokumentacji medycznej. W odniesieniu do dokumentacji prowadzonej przez psychologów należy zauważyć, że znacznie szersze uregulowania zawierają przepisy z zakresu medycyny pracy, tj. ustawy z dnia 27 czerwca 1997 r. o służbie medycyny pracy (t. j. Dz. U. Nr 125, poz. 1317 z 2004 r.) oraz wydane na jej podstawie rozporządzenie Ministra Zdrowia z dnia 14 lipca 2010 r. w sprawie rodzajów dokumentacji badań i orzeczeń psychologicznych, sposobu jej prowadzenia, przechowywania i udostępniania oraz wzorów stosowanych dokumentów (Dz. U. Nr 131, poz. 888). Przepisy te w sposób szczegółowy określają rodzaje oraz sposób prowadzenia dokumentacji przez psychologów w związku z zadaniami wykonywanymi przez nich w ramach służby medycyny pracy. Zgodnie z art. 11 ust. 3 powołanej ustawy, dane zawarte w dokumentacji medycznej oraz dane zawarte w dokumentacji, o której mowa w ust. 2a, są objęte tajemnicą zawodową i służbową. Dane te mogą być udostępniane wyłącznie podmiotom określonym w art. 19 i art. 2 ust. 4 oraz podmiotom uprawnionym do udostępniania im dokumentacji medycznej na podstawie i zasadach określonych w odrębnych przepisach. Stosownie do art. 2a obowiązek prowadzenia dokumentacji badań i orzeczeń psychologicznych obejmuje również psychologa, o którym mowa w art. 2 ust. 3 pkt 2. Sygnalizowane w niniejszym wystąpieniu zagadnienie miało o tyle istotne znaczenie, że dokumentacja usług psychologicznych zawiera w wielu przypadkach dane wrażliwe, wymienione w art. 27 ust. 1 (np. dane o stanie zdrowia, nałogach, życiu seksualnym, dane dotyczące skazań), którym ustawa o ochronie danych osobowych danym zapewnia wysoki reżim ochrony. Na mocy art. 27 ustawy o ochronie danych osobowych przetwarzanie tej kategorii danych jest co do zasady zabronione, z wyjątkiem przypadków enumeratywnie wyliczonych w art. 27 ust. 2 ustawy. Generalny Inspektor podkreślił, że rozporządzenie może jedynie konkretyzować regulacje ustawowe, nie zaś stanowić samoistną podstawę dla przetwarzania danych tzw. szczególnie chronionych. W świetle powyższego Generalny Inspektor zwrócił się z prośbą o podjęcie prac legislacyjnych w celu precyzyjnego uregulowania sposobu prowadzenia dokumentacji prowadzonej przez psychologów, w tym określenia wprost, że osoba, której dokumentacja dotyczy (klient korzystający z usług psychologicznych), jest uprawniona do wglądu do

tej dokumentacji. W ten sposób wyeliminowane zostaną przypadki bezzasadnych naruszeń praw osób korzystających z takich usług, do kontroli procesu przetwarzania dotyczących ich danych. Generalny Inspektor zauważył, że wzór dla stosownych zmian w omawianym zakresie mogłyby stanowić odpowiednie regulacje dotyczące dokumentacji medycznej, w tym wspomnianej ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w szczególności art. 26 i 27 tej ustawy oraz rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. Nr 252, poz. 1697). Do przepisów tych nawiązują również wskazane powyżej przepisy ustawy o służbie medycyny pracy.

W odpowiedzi Minister Pracy i Polityki Społecznej podzielił uwagi Generalnego Inspektora dotyczące uregulowania przedmiotowej kwestii. Niemniej jednak informacyjnie warto zaznaczyć, że w dniu 27 września 2012 r. do Biura GODO w wpłynął projekt ustawy o uchyleniu ustawy o zawodzie psychologa i samorządzie zawodowym psychologów oraz niektórych innych ustaw. W odniesieniu do przedstawionego projektu Generalny Inspektor wskazał, że organ do spraw ochrony danych osobowych nie jest władny rozstrzygać, czy uzasadnione jest całkowite uchylenie ustawy o zawodzie psychologa i samorządzie zawodowym psychologów, czy jedynie podjęcie prac zmierzających do poprawienia tego aktu prawnego. Skoro jednak projektodawca przyjął to pierwsze rozwiązanie, Generalny Inspektor Ochrony Danych Osobowych przypomniał, że w piśmie z dnia 11 kwietnia 2012 roku (znak: DDP-I-4321-39-MW/KW/2012, L.dz. 1003/12) Minister Pracy i Polityki Społecznej zobowiązał się rozważyć przygotowanie nowej regulacji, która z jednej strony – umożliwiałaby łatwiejszy dostęp do zawodu psychologa, z drugiej zaś – zapewniała zgodność z regulacjami ustawy o ochronie danych osobowych, w tym – wskazanymi w wystąpieniu Generalnego Inspektora Ochrony Danych Osobowych – unormowaniami statuującymi określone uprawnienia osób, których dane psychologowie będą przetwarzać.

**O podjęcie prac legislacyjnych mających na celu prawne uregulowanie zasad i sposobu prowadzenia dokumentacji przez rodzinne ośrodki diagnostyczne-konsultacyjne**<sup>222</sup> zwrócił się GODO do Ministra Sprawiedliwości w wystąpieniu z **dnia 2 kwietnia 2012 r.** Powodem tego wystąpienia były sygnalizowane Generalnemu Inspektorowi wątpliwości i zastrzeżenia dotyczące przypadków odmawiania osobom, których dane dotyczą lub ich przedstawicielom ustawowym, dokumentacji badań przeprowadzanych przez rodzinne ośrodki diagnostyczno-konsultacyjne. Wobec braku szczegółowych regulacji dotyczących zasad i sposobu prowadzenia, w tym udostępniania dokumentacji przez te podmioty, zwrócił się więc z prośbą do Ministra Sprawiedliwości o rozwiązanie powyższego problemu poprzez dokonanie zmian odpowiednich przepisów prawa. Celem tych zmian miałyby być prawne uregulowanie sposobu prowadzenia, udostępniania i przechowywania, w tym

---

<sup>222</sup> DOLiS-035-993/12/21309

terminów przechowywania przedmiotowej dokumentacji, jak również określenie sposobu postępowania z dokumentacją w razie ewentualnej likwidacji ośrodka diagnostyczno-konsultacyjnego. Jak zauważył Generalny Inspektor, przepisy rozporządzenia Ministra Sprawiedliwości z dnia 3 sierpnia 2001 r. w sprawie organizacji i zakresu działania rodzinnych ośrodków diagnostyczno-konsultacyjnych (Dz. U. Nr 97, poz. 1063), w tym w szczególności § 12, odnoszą się jedynie do rodzajów dokumentacji prowadzonej przez te ośrodki. Nie regulują one natomiast szczegółowych zasad postępowania z tą dokumentacją. Generalny Inspektor wskazał zatem, że w praktyce zdarzają się sytuacje, w których powstają istotne wątpliwości, w jaki sposób dokumentacja w postaci protokołów działań merytorycznych, przeprowadzonych wywiadów, testów, obserwacji, porad, mediacji oraz kopie sporządzonych opinii, miałyby być przechowywana oraz komu i w jaki sposób udostępniana. W sprawach sygnalizowanych Generalnemu Inspektorowi opisywano zdarzenia, w których kierownicy rodzinnych ośrodków diagnostyczno-konsultacyjnych odmawiali osobom, wobec których badania były przeprowadzane, udostępniania prowadzonej dokumentacji. Jako uzasadnienie odmowy podawano, że *„dokumentacja taka jest materiałem roboczym służącym biegłym do opracowania opinii i czytelnym tylko dla nich; poza tym testy psychologiczne mogą być udostępniane wyłącznie specjalistom”*. W ten sposób naruszane były konstytucyjnie gwarantowane prawa osób, których przedmiotowa dokumentacja dotyczyła. Konstytucja RP stanowi bowiem, że każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Generalny Inspektor przypomniał, że ograniczenie tego prawa może określić jedynie ustawa (art. 51 ust. 3 Konstytucji RP). Zdaniem Generalnego Inspektora, precyzyjne uregulowanie sposobu prowadzenia dokumentacji prowadzonej przez ośrodki diagnostyczno-konsultacyjne, w tym określenie wprost, że osoba, której dokumentacja dotyczy, jest uprawniona do jej wglądu, przyczyni się do wyeliminowania przypadków bezzasadnej i istotnie naruszającej prawa osób poddawanych badaniom, odmowy udostępniania dotyczących ich dokumentów. Wzór dla stosownych zmian w tym zakresie mogłyby stanowić odpowiednie regulacje dotyczące dokumentacji medycznej, zawarte w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.), w szczególności w art. 26 i 27 tej ustawy oraz rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. Nr 252, poz. 1697). Generalny Inspektor zaznaczył też, że w przypadku danych wrażliwych, wymienionych w art. 27 ust. 1 ustawy o ochronie danych osobowych, zapewniony jest wysoki reżim ich ochrony. Wobec jednoznacznej dyspozycji art. 27 ust. 2 pkt 2 tej ustawy, gdyby podstawę dla przetwarzania danych sensytywnych miałby stanowić przepis ustawy, musiałby on spełniać określone w tym punkcie kryteria. Zgodnie z art. 27 ust. 2 pkt 2 ustawy, 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. W celu zapewnienia takich gwarancji normy ustawowe powinny określać zakres danych, podmioty uprawnione do ich przetwarzania oraz szczegółowe zasady postępowania z danymi, ich udostępniania, czasu ich przechowania, a także sposobu postępowania z dokumentacją po zakończeniu działalności ośrodka. Jak zauważył Generalny Inspektor rozporządzenie natomiast może jedynie konkretyzować regulacje ustawowe, nie zaś stanowić samoistną podstawę dla przetwarzania danych tzw. szczególnie chronionych.

W odpowiedzi Minister Sprawiedliwości wskazał, że przygotowany został projekt założeń ustawy o zmianie ustawy o postępowaniu w sprawach nieletnich i ustawy – Prawo o ustroju sądów powszechnych, który przekazano do konsultacji społecznych i uzgodnień międzyresortowych. Ponadto w odpowiedzi podniesiono argument, że przedmiotowe przepisy niewątpliwie wymagają wprowadzenia stosownych zmian.

Kolejne prezentowane wystąpienie miało na celu **zmianę aktualnego stanu prawnego wynikającego z przepisów art. 23c ust. 3 ustawy z dnia 26 czerwca 2003 r. o ochronie prawnej odmian roślin (Dz. U. Nr 137, poz. 1300 z późn. zm.), zezwalającego na przeprowadzanie kontroli zgodności informacji dotyczącej wykorzystania materiału ze zbioru odmiany chronionej wyłącznym prawem, jako materiału siewnego, ze stanem faktycznym - hodowcom, organizacjom hodowców albo osobom upoważnionym na podstawie pełnomocnictwa, bez ustawowego określania zakresu przetwarzanych w nim i dla jego potrzeb danych osobowych.**

Impulsem do wystosowania w dniu 12 kwietnia 2012 r. wystąpienia<sup>223</sup> w tej sprawie do Ministra Rolnictwa i Rozwoju Wsi było pozyskanie przez Generalnego Inspektora Ochrony Danych Osobowych informacji o działaniach podejmowanych przez Agencję Nasienną sp. z o. o. z siedzibą w Lesznie, polegających na wzywaniu rolników do składania sprawozdań zawierających ich dane osobowe bez podania celu, w jakim mają to czynić. Po przeanalizowaniu przepisów ustawy o ochronie prawnej odmian roślin, wątpliwości Generalnego Inspektora wzbudziła treść art. 23c ww. ustawy w zakresie, w jakim zezwala hodowcom albo organizacjom hodowców, albo osobom upoważnionym na podstawie pełnomocnictwa przez hodowcę albo organizację hodowców, do przeprowadzania kontroli. Generalny Inspektor powołał art. 23a ust. 1<sup>224</sup> oraz 23a ust. 3<sup>225</sup> ustawy o ochronie prawnej odmian roślin i uznał, że zastosowanie w art. 23a ust. 2<sup>226</sup> zwrotu „w szczególności” powoduje, iż wniosek o przekazywanie

---

<sup>223</sup> DOLiS-035-327/12/23743

<sup>224</sup> Posiadacz gruntów rolnych, z wyłączeniem posiadacza gruntów rolnych określonego w art. 23 ust. 3, albo organizacja reprezentująca posiadaczy gruntów rolnych, przekazuje hodowcom albo organizacjom hodowców, na ich wniosek, pisemną informację dotyczącą wykorzystania materiału ze zbioru, o którym mowa w art. 23 ust. 2 pkt 1, jako materiału siewnego, w terminie 30 dni od dnia otrzymania wniosku.

<sup>225</sup> Sposób oraz zakres udzielania informacji, o której mowa w ust. 1, są ustalane w umowie określonej w art. 23 ust. 4.

<sup>226</sup> Wniosek, o którym mowa w ust. 1, zawiera w szczególności: 1) imię i nazwisko oraz adres miejsca zamieszkania albo nazwę i adres siedziby hodowcy; 2) wskazanie: a) odmiany lub odmian, w odniesieniu do których hodowca albo organizacja hodowców wnioskują o udzielenie informacji, b) wysokości opłaty licencyjnej dla poszczególnych odmian roślin, o których mowa w lit. a.

pisemnej informacji dotyczącej wykorzystania materiału siewnego odmian roślin określonych w ustawie, może zawierać jeszcze inne rodzaje danych i tym samym stwarzać ryzyko pozyskiwania dodatkowych danych osobowych niewymienionych w przepisach ustawy. Generalny Inspektor stanął na stanowisku, iż uprawnienie do pozyskiwania innych danych niż określone we wniosku, nie powinno być stosowane rozszerzająco przez hodowców lub organizacje hodowców, a w odniesieniu do danych osobowych wykraczać poza katalog danych określonych w ust. 2 pkt 1 ustawy o ochronie prawnej roślin. Generalny Inspektor zwrócił się zatem z prośbą o rozważenie zmiany wskazanych przepisów ustawy poprzez rezygnację z posługiwania się zwrotem „w szczególności” w odniesieniu do pozyskiwanych w ten sposób danych osobowych i tym samym stworzenie ich zamkniętego katalogu. W przypadku niezawarcia umowy Generalny Inspektor podniósł, że informacja dotycząca wykorzystania materiału ze zbioru materiału siewnego odmiany chronionej zawiera dane z art. 23a ust. 4<sup>227</sup> ustawy o ochronie prawnej odmian roślin. Wówczas uprawnienia kontrolne, zgodnie z art. 23c ust. 3 ustawy o ochronie prawnej odmian roślin, przysługują oprócz hodowcy i organizacji hodowców również osobie upoważnionej na podstawie pełnomocnictwa przez hodowcę albo organizację hodowców. Zdaniem Generalnego Inspektora, o ile kwestie uprawnień kontrolnych przyznanych hodowcom i organizacjom hodowców, regulowane w art. 23c ustawy o ochronie prawnej odmian roślin, nie dotyczące ochrony danych osobowych, wykraczają poza kompetencje Generalnego Inspektora Ochrony Danych Osobowych, to jego wątpliwości wzbudza przepis ust. 3 tego artykułu w zakresie, w jakim kontrola sposobu wykorzystania materiału ze zbioru była dokonywana przez osobę upoważnioną przez hodowcę albo organizację hodowców na podstawie pełnomocnictwa o nieznanym zakresie przetwarzanych dla jego potrzeb danych osobowych. Generalny Inspektor wyraźnie podkreślił, że ustawa nie precyzuje w jakim zakresie, w jaki sposób oraz dla jakich celów pozyskiwane i wykorzystywane były dane osobowe osób przeprowadzających kontrolę oraz osób kontrolowanych przez hodowcę albo organizację hodowców. Zaznaczył również, iż każdy podmiot przetwarzający dane osobowe jest obowiązany do stosowania przepisów ustawy o ochronie danych osobowych na każdym etapie przetwarzania tych danych, jak w sytuacji zbierania, przechowywania czy udostępniania, o ile przepisy innych aktów prawnych nie określają w sposób szczególny tego przetwarzania. Jak przypomniał Generalny Inspektor, ustawa o ochronie danych osobowych wymaga, aby dane osobowe

---

<sup>227</sup> Jeżeli umowa określona w art. 23 ust. 4 nie została zawarta, informacja, o której mowa w ust. 1, zawiera: 1) imię i nazwisko oraz adres miejsca zamieszkania albo nazwę i adres siedziby posiadacza gruntów rolnych; 2) dane umożliwiające identyfikację działek rolnych, w rozumieniu przepisów o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności, wchodzących w skład gospodarstwa rolnego posiadacza gruntów rolnych; 3) oświadczenie posiadacza gruntów rolnych o wykorzystaniu bądź niewykorzystaniu materiału ze zbioru, o którym mowa w art. 23 ust. 2 pkt 1, jako materiału siewnego wraz z podaniem nazw odmian, w stosunku do których wyłączne prawo posiada hodowca; 4) <sup>(27)</sup> wskazanie ilości materiału ze zbioru, o którym mowa w art. 23 ust. 2 pkt 1, wykorzystanego jako materiał siewny, oraz wielkości powierzchni gruntów rolnych, na której materiał ten został użyty; 5) imię i nazwisko oraz adres miejsca zamieszkania albo nazwę i adres siedziby przetwórcy, który wykonał dla posiadacza gruntów rolnych usługę przygotowania do rozmnażania materiału ze zbioru, o którym mowa w art. 23 ust. 2 pkt 1, na materiał siewny; 6) imię i nazwisko oraz adres miejsca zamieszkania albo nazwę i adres siedziby podmiotu, od którego posiadacz gruntów rolnych nabył kwalifikowany materiał siewny odmiany lub odmian, o których mowa w ust. 2 pkt 2 lit. a, wraz ze wskazaniem ilości tego materiału.

były adekwatne w stosunku do celów, dla jakich są przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Dane swym rodzajem i treścią nie powinny wykraczać poza potrzeby wynikające z celu ich przetwarzania. Administrator danych może zatem przetwarzać jedynie takie dane, które są niezbędne do osiągnięcia zamierzonego celu. Ocena przywołanej zasady adekwatności należy do projektodawcy, który tworząc zamknięty katalog danych osobowych jakie ma zawierać określony dokument, powinien wskazać wyłącznie dane niezbędne dla celu jego sporządzenia. Ustanowienie odpowiednich przepisów ustawy o ochronie prawnej odmian roślin nie tylko wyeliminuje wątpliwości dotyczące zakresu danych przetwarzanych w dokumencie pełnomocnictwa do przeprowadzenia kontroli, ale również przyczyni się do ochrony praw osób, których dane dotyczą.

W odpowiedzi na wystąpienie Generalnego Inspektora, Minister Rolnictwa i Rozwoju Wsi wskazał potrzebę analizy w/w argumentacji i zobowiązał się wziąć pod uwagę przedstawione stanowisko dotyczące konieczności zmiany zakwestionowanych przepisów prawa.

Na uwagę zasługuje wystąpienie Generalnego Inspektora z dnia 17 kwietnia 2012 r.<sup>228</sup> do **Prezesa Naczelnej Rady Lekarskiej, z prośbą o zasygnalizowanie członkom samorządu lekarskiego konieczności respektowania prawa do prywatności oraz ochrony informacji związanych z pacjentem podczas wykonywania praktyk lekarskich, jak również organizowania obsługi pacjentów, w szczególności w sytuacjach rejestrowania pacjentów na wizyty lekarskie, wydawania im wyników badań, ustalania harmonogramu zabiegów w sanatoriach, wywoływania do gabinetów lekarskich lekarzy specjalistów, itp.** Generalny Inspektor przypomniał, że jako organ ochrony danych osobowych wielokrotnie otrzymuje pisma zawierające zastrzeżenia i wątpliwości pacjentów dotyczące sposobu wykonywania powyższych czynności. W pismach tych podawane były przypadki konieczności przekazywania przez pacjentów bardzo szczegółowych informacji pozwalających na identyfikację osoby wraz ze szczegółowymi informacjami o stanie ich zdrowia, np. w obecności wielu innych osób oczekujących w kolejce do rejestracji lub na wizytę lekarską. Takie warunki wykonywania wymienionych czynności niewątpliwie narażają pacjentów na naruszenie ich praw lub stanowią takie naruszenie. Tego rodzaju sytuacjom można zaradzić poprzez przyjęcie pewnych rozwiązań organizacyjnych, stosowanych w niektórych przychodniach, gdzie zapisy na wizyty, badania, czy zabiegi odbywają się np. w oddzielnym pomieszczeniu lub przy stanowiskach, przy których obsługiwany pacjent znajduje się w pewnej odległości od reszty osób oczekujących. Przy wzywaniu do gabinetu lekarskiego przyjmowany jest np. sposób wywoływania jedynie po imieniu pacjenta, godzinie zapisu lub numerze, pod którym pacjent został zarejestrowany. Generalny Inspektor przypomniał, że prywatność pacjentów chroniona jest m. in. przez ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz ustawę z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku

---

<sup>228</sup> DOLiS-035-1188/12/24644

Praw Pacjenta. Konieczność poszanowania prawa do intymności i godności pacjenta wynika w szczególności z przepisów art. 13 i 14 ww. ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Przepisy te stanowią, że pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, uzyskanych w związku z wykonywaniem zawodu medycznego. Generalny Inspektor wskazał, że obowiązek ten wynika również z przepisów innych ustaw, np. 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. 2009 r. Nr 151 poz. 1217 z późn. zm.), ustawy z dnia 20 lipca 1950 r. o zawodzie felczera (t. j. Dz. U. 2004 r. Nr 53 poz. 531 z późn. zm.), a także Kodeksu Etyki Lekarskiej. Ponadto przypomniał, że dane o stanie zdrowia są danymi szczególnie chronionymi, których przetwarzanie - co do zasady - jest zabronione. Art. 27 ust. 2 pkt 7 ustawy dopuszcza przetwarzanie danych szczególnie chronionych, w tym danych o stanie zdrowia, gdy jest to prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych. Powoływanie się na ten przepis uprawnione jest jedynie w odniesieniu do realizacji wymienionych celów i nie może następować w celu uzasadniania udostępniania tych danych innym osobom. Rozumiejąc potrzebę ochrony stanu zdrowia, Generalny Inspektor wskazał, że osobie chorej przysługuje także prawo do ochrony jej sfery życia prywatnego, zwłaszcza gdy dotyczy to danych szczególnie chronionych. Generalny Inspektor powołał zasady wynikające z art. 26 ust. 1 pkt 1 - pkt 3 ustawy o ochronie danych osobowych i zaapelował o to, aby w trosce o poszanowanie praw do prywatności pacjentów i ochronę informacji ich dotyczących, stosować jedynie takie rozwiązania, które pozostają w zgodzie z powyżej powołanymi przepisami.

W odpowiedzi Prezes Naczelnej Rady Lekarskiej wykazał zrozumienie wobec argumentacji Generalnego Inspektora i obiecał podjąć odpowiednie działania.

Adresatem kolejnych czterech wystąpień Generalnego Inspektora Ochrony Danych Osobowych był **Minister Zdrowia**. Jedno z nich, a mianowicie wystąpienie z dnia 31 stycznia 2012 r.<sup>229</sup> związane było z zasygnalizowanym Generalnemu Inspektorowi Ochrony Danych Osobowych problemem nałożenia na lekarzy - mocą znowelizowanego rozporządzenia Ministra Zdrowia z dnia 7 stycznia 2004 r. w sprawie badań lekarskich kierowców i osób ubiegających się o uprawnienia do kierowania pojazdami (Dz. U. z 2004 r. Nr 2, poz. 15) - obowiązku przekazywania danych o stanie zdrowia właściwym organom administracji. Zgodnie z załącznikiem nr 3 pkt 2 tego rozporządzenia, na lekarzy, którzy podczas wykonywania zawodu

---

<sup>229</sup> DOLiS-035-2167-11

stwierdzą u osoby ubiegającej się o prawo jazdy lub posiadającej prawo jazdy, przypadek wystąpienia epizodu ciężkiej hipoglikemii, niezależnie od okoliczności, został nałożony obowiązek niezwłocznego powiadomienia organu wydającego prawo jazdy o konieczności dokonania oceny predyspozycji zdrowotnych tej osoby do kierowania pojazdami. Załącznik nr 4 pkt 4 powołanego rozporządzenia nakłada natomiast na lekarzy obowiązek niezwłocznego powiadomienia organu wydającego prawo jazdy o konieczności dokonania oceny predyspozycji zdrowotnych tej osoby do kierowania pojazdami w sytuacji, w której podczas wykonywania zawodu, niezależnie od okoliczności, stwierdzą oni u osoby ubiegającej się o prawo jazdy lub posiadającej prawo jazdy, przypadek wystąpienia napadu o symptomatologii padaczkowej lub podejrzenie albo istnienie padaczki.

Biorąc pod uwagę kierowane do Generalnego Inspektora zastrzeżenia przedstawicieli zawodów medycznych, dbałość o przestrzeganie zasad prawidłowej legislacji, jak i poszanowanie praw osób, których danych dotyczą, szczególnie w tak newralgicznym obszarze, jakim jest przetwarzanie danych o stanie zdrowia, organ do spraw ochrony danych osobowych wskazał, iż rozwiązanie prawne przyjęte w powołanym rozporządzeniu nie tylko nie mieści się w zakresie delegacji ustawowej przewidzianej w art. 123 ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym (Dz. U. z 2005 r. Nr 108, poz. 908 z późn. zm.) i w art. 81 mającej wejść w życie ustawy o kierujących pojazdami, ale również - co najistotniejsze - budzi zasadnicze wątpliwości co do zgodności z Konstytucją Rzeczypospolitej Polskiej, przepisami statuującymi tajemnicę informacji związanych z pacjentem, określoną przede wszystkim w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.), jak również z przepisami o ochronie danych osobowych.

Generalny Inspektor wskazał, że Konstytucja w art. 47 statuuje prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Zgodnie z art. 51 ust. 1 i 5 Konstytucji RP nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a zasady i tryb gromadzenia oraz udostępniania informacji dotyczących osoby powinna określać ustawa. Ograniczenia w zakresie korzystania z prawa do ochrony życia prywatnego i decydowania o swoim życiu osobistym wymagają bezwzględnie regulacji rangi ustawowej (art. 31 ust. 3 Konstytucji RP). Przypomnieć w tym miejscu wypada, że Trybunał Konstytucyjny w cytowanym już wcześniej uzasadnieniu postanowienia z dnia 31 stycznia 2007 roku (sygn. akt S 1/2007) stwierdził: „Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować” funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. Także art. 31 ust. 3 Konstytucji

*Rzeczypospolitej Polskiej wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki".*

Art. 31 Konstytucji statuuje tzw. zasadę proporcjonalności. Godząc się na limitowanie konstytucyjnych praw i wolności, ustawodawca precyzuje warunki dopuszczalności tego rodzaju ograniczeń. Trybunał Konstytucyjny w swym orzecznictwie wielokrotnie wskazywał, że art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej precyzyjnie określa przesłanki dopuszczalności ograniczeń w korzystaniu z wolności i praw jednostki. Należą do nich: a) ustawowa forma ograniczeń, b) funkcjonalny związek ograniczenia z realizacją wartości wskazanych enumeratywnie w art. 31 ust. 3 Konstytucji, c) istnienie konieczności ograniczeń, przy braku innych środków skutecznie służących temu celowi, d) zakaz naruszania istoty danej wolności lub prawa<sup>230</sup>.

Obowiązek niezwłocznego powiadomienia organu wydającego prawo jazdy o konieczności dokonania oceny predyspozycji zdrowotnych osoby do kierowania pojazdami, budzi zastrzeżenia przede wszystkim ze względu na istnienie tajemnicy zawodowej, określonej w art. 13 i 14 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Obowiązek zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku 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. 2009 r. Nr 151 poz. 1217 z późn. zm.), ustawy z dnia 20 lipca 1950 r. o zawodzie felczera (t.j. Dz. U. 2004 r. Nr 53 poz. 531 z późn. zm.) oraz - co podnoszą zgłaszający swoje zastrzeżenia w tym zakresie przedstawiciele podmiotów prowadzących działalność leczniczą - Kodeksem etyki lekarskiej. Wskazać również należy, że zgodnie z art. 5 ustawy o ochronie danych osobowych, jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę niż wynika to z przywołanej wyżej ustawy, stosuje się przepisy tych ustaw. Nałożenie na podmioty związane tajemnicą zawodową obowiązku ujawniania organowi wydającemu prawo jazdy informacji objętych tą tajemnicą, w określonej sytuacji wymaga istnienia przepisu rangi ustawy, który by na takie działanie wprost zezwalał. Prawidłowo skonstruowana podstawa prawna dla przekazywania innemu podmiotowi danych pacjenta objętych tajemnicą zawodową, powinna ściśle określać warunki, zakres i sposób takiego udostępnienia. Ponadto niezbędne jest wprowadzenie dodatkowego przepisu rozciągającego obowiązek zachowania powyższej tajemnicy na podmioty, którym informacje te będą przekazywane. Jedynie w ten sposób zapewnione zostałyby gwarancje ochrony prywatności pacjentów i zachowania tajemnicy informacji uzyskiwanych w związku z wykonywaniem zawodu medycznego.

---

<sup>230</sup> Wyrok Trybunału Konstytucyjnego z dnia 15 grudnia 2004 r. K. 2/2004 OTK ZU 2004/11A poz. 117; por. też np. wyrok TK z dnia 29 czerwca 2001 r. K. 23/2000 OTK ZU 2001/5 poz. 124, wyrok z dnia 12 stycznia 2000 r. P. 11/98 OTK ZU 2000/1 poz. 3.

W odpowiedzi Minister Zdrowia pismem z dnia 17 lipca 2012 r. wskazał, że obowiązek informowania przez lekarza odpowiednich organów o występowaniu przeciwwskazań zdrowotnych do kierowania pojazdami, będzie wynikał wprost z treści art. 79 ust. 8 ustawy o kierujących pojazdami, którego wejście w życie nastąpiło w dniu 1 stycznia 2013 r.

Z kolei w wystąpieniu z dnia 6 marca 2012 r.<sup>231</sup> **Generalny Inspektor Ochrony Danych osobowych wskazywał Ministrowi Zdrowia na potrzebę podjęcia prac legislacyjnych mających na celu określenie jednolitego wzoru legitymacji Honorowego Dawcy Krwi, ze szczególnym uwzględnieniem zakresu zawartych w tym dokumencie informacji.** Pozwoliłoby to wyeliminować praktykę nadmiernej i niejednokrotnie zbędnej ingerencji w prywatność osób oddających krew - Honorowych Dawców Krwi. Generalny Inspektor wskazał, że powyższy problem ujawnił się na tle sygnalizowanych wątpliwości honorowych dawców, którzy aby móc skorzystać ze zwolnień w opłatach za podróżowanie środkami transportu zbiorowego zmuszeni byli do okazywania legitymacji Honorowego Dawcy Krwi i ujawniania danych w niej zawartych. Generalny Inspektor powołał art. 6 ust. 1<sup>232</sup> oraz art. 7 ust. 1<sup>233</sup> ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. 1997 r. Nr 106 poz. 681 z późn. zm.) i stwierdził, że w przeciwieństwie do legitymacji „Honorowego Zasłużonego Dawcy Krwi” – której wzór określa rozporządzenie Ministra Zdrowia z dnia 21 sierpnia 2006 r. w sprawie określenia wzoru oraz szczegółowych zasad i trybu nadawania odznaki honorowej „Zasłużony Honorowy Dawca Kwi” – wzór legitymacji „Honorowego Dawcy Krwi” nie został określony w żadnym z aktów prawnych. Uznał również, że prowadzi to do sytuacji, iż każda z jednostek organizacyjnych publicznej służby krwi, która wydaje legitymację „Honorowego Dawcy Krwi”, sama ustala jej wzór oraz w sposób dowolny umieszcza w niej zakres danych osobowych, w tym szczególnie chronionych. Zdaniem Generalnego Inspektora szczególne zastrzeżenia budziło to, iż za pomocą przedmiotowej legitymacji w poszczególnych jednostkach organizacyjnych publicznej służby krwi, udostępniane były dane osobowe honorowych dawców w niejednakowym i w zbyt szerokim zakresie, co często stanowiło nadmierną ingerencję w prywatność tych osób. Zdarzały się przypadki, że w legitymacjach umieszczane były takie informacje o osobie, jak np. grupa krwi. Ze względu na szeroko rozumiane pojęcie „dane o stanie zdrowia”, jakim posługują się przepisy art. 27 ustawy o ochronie danych osobowych wprowadzające szczególny reżim przetwarzania danych tzw. wrażliwych, Generalny Inspektor wskazał, że informację tę należy zaliczyć do danych szczególnie chronionych, a co za tym idzie, jej przetwarzanie jest możliwe jedynie w przypadku spełnienia przez administratora danych jednej z przesłanek określonych w art. 27 ust. 2 pkt 1 – 10 wspomnianej ustawy.

---

<sup>231</sup> DOLiS-035-637/12/14306

<sup>232</sup> Osobie, która oddała bezpłatnie krew i została zarejestrowana w jednostce organizacyjnej publicznej służby krwi, przysługuje tytuł "Honorowy Dawca Krwi".

<sup>233</sup> Honorowy dawca krwi otrzymuje legitymację "Honorowego Dawcy Krwi", wydaną przez jednostkę organizacyjną publicznej służby krwi.

Ponadto w świetle brzmienia art. 13 ust. 1<sup>234</sup> ustawy o publicznej służbie krwi, administrator danych powinien przetwarzać w zgodzie z obowiązującym prawem tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel ich zbierania. GODO zwrócił również uwagę na zasady prawidłowego przetwarzania danych osobowych wyrażonych w art. 26 ust. 1-3 ustawy i przypomniał, że zasada zgodnego z prawem przetwarzania danych osobowych oznacza konieczność niewykraczania poza odpowiednie regulacje ustawowe, czy wynikające z innych źródeł prawa powszechnie obowiązującego. Administrator danych nie może przetwarzać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem stopniu szczegółowości<sup>235</sup>. W sytuacji umieszczenia w legitymacji „Honorowego Dawcy Krwi” danych w szerszym zakresie niż było to niezbędne dla celu, w jakim wydaje się przedmiotowy dokument, dalsze posługiwanie się legitymacją prowadziło do ujawnienia danych osobowych honorowych dawców krwi w nieadekwatnym zakresie. W opinii Generalnego Inspektora wydaje się konieczne wprowadzenie do aktów wykonawczych wydanych na podstawie delegacji z ustawy o publicznej służbie krwi, regulacji określających jednolity dla wszystkich jednostek organizacyjnych publicznej służby, wzór legitymacji „Honorowego Dawcy Krwi”. Jak zauważył Generalny Inspektor, przy opracowywaniu wzoru legitymacji można opierać się na przepisach stanowiących o wzorach legitymacji „Honorowego Zasłużonego Dawcy Krwi”, które zawierają jedynie niezbędne dane osobowe.

Na dzień sporządzenia przedmiotowego *Sprawozdania*, wskazany problem był nadal aktualny. Nad jego rozwiązaniem organ do spraw ochrony danych osobowych współpracuje z Ministerstwem Zdrowia oraz Narodowym Funduszem Zdrowia.

Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu do **Ministra Zdrowia z dnia 27 marca 2012 r. zwrócił się z prośbą o zasygnalizowanie podmiotom prowadzącym działalność leczniczą potrzeby wyeliminowania praktyki umieszczania przy łózkach pacjentów kart gorączkowych, zawierających dane osobowe w zakresie: imienia, nazwiska pacjenta oraz rozpoznania jego choroby, w sposób umożliwiający zapoznanie się z treścią kart osobom do tego nieuprawnionym**<sup>236</sup>. Stosowany powszechnie w szpitalach sposób umieszczania kart gorączkowych przy łózkach pacjentów prowadził do sytuacji, w której dane o stanie zdrowia pacjentów, a zatem dane szczególnie chronione, dostępne były dla osób trzecich (np. odwiedzających chorych), co w istotny sposób godziło w prawo do prywatności pacjentów oraz prawo do ochrony dotyczących ich danych osobowych. Problem ten miał większe znaczenie w przypadkach umieszczania kart gorączkowych

---

<sup>234</sup> Publiczna służba krwi zapewnia anonimowość dawcy krwi.

<sup>235</sup> Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r., sygn. akt II SA/Wa 917/2005.

<sup>236</sup> DOLiS-035- 995/12



w salach oddziałów ogólnodostępnych dla odwiedzających, niż w oddziałach o szczególnym nadzorze medycznym (np. OIOM), gdzie dostęp takich osób był z zasady ograniczony.

Obowiązujące przepisy prawa regulują na zasadach ogólnych zasady dostępu do dokumentacji medycznej zawierającej dane osobowe pacjenta, w tym dane szczególnie chronione, jak również odnoszą się do kwestii prowadzenia karty gorączkowej hospitalizowanej osoby. Nie regulują jednak sposobu umieszczania karty gorączkowej przy łóżku pacjenta. Rozumiejąc potrzebę ochrony stanu zdrowia wskazać jednakże należy, że osobie chorej przysługuje także prawo do ochrony jej sfery życia prywatnego, zwłaszcza gdy dotyczy to danych szczególnie chronionych, jakimi są dane o jej stanie zdrowia. W swoim wystąpieniu Generalny Inspektor wskazał, że w świetle przepisów prawa, w tym przepisów o ochronie danych osobowych, brak jest uzasadnienia dla zamieszczenia danych osobowych, w tym szczególnie chronionych, w treści karty gorączkowej tak, aby były dostępne dla osób do tego nieupoważnionych. Podkreślił szczególny charakter danych o stanie zdrowia w świetle art. 27 ust. 1 ustawy o ochronie danych osobowych, a także wskazał, że powoływanie się na art. 27 ust. 2 pkt 7 wskazanej ustawy uprawnione jest jedynie w odniesieniu do realizacji wymienionych w tym przepisie celów i nie może następować w celu uzasadniania udostępniania tych danych innym osobom.

W omawianym przypadku nie sposób również przyjąć, iż spełnione były określone w art. 26 ust. 1 pkt 1 - pkt 3 ustawy zasady: legalizmu, celowości i adekwatności przetwarzania danych oraz zagwarantowane było bezpieczeństwo danych. Realizacja obowiązku właściwego zabezpieczenia danych osobowych oznacza między innymi przyjęcie takiego sposobu przetwarzania danych, który wyeliminuje możliwość zapoznania się z danymi przez osoby do tego nieupoważnione. Generalny Inspektor wskazał również na istnienie tajemnicy określonej w art. 13 i 14 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417 z późn. zm.). Przepis ten stanowi, że pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, uzyskanych w związku z wykonywaniem zawodu medycznego. Zgodnie z art. 14, 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 ich zdrowia. Mając powyższe na uwadze Generalny Inspektor zaapelował, aby podmioty wykonujące działalność leczniczą, w trosce o poszanowanie prawa do prywatności pacjentów i ochronę informacji ich dotyczących, stosowały jedynie takie rozwiązania, które pozostają w zgodzie z powyżej powołanymi przepisami np. poprzez przesłonięcie bądź odwrócenie tej karty, całkowite zrezygnowanie z umieszczania jej przy łóżku pacjenta, bądź przyjęcie innego sposobu przechowywania tego rodzaju dokumentacji medycznej.

W odpowiedzi Minister Zdrowia poinformował, że wystąpił do dyrektorów podmiotów leczniczych prowadzących szpitale z prośbą o zwrócenie szczególnej uwagi na realizację praw pacjenta w przedmiotowym zakresie.

Natomiast wystąpienie Generalnego Inspektora z dnia **12 czerwca 2012 r. do Ministra Zdrowia** zawierało prośbę o podjęcie prac legislacyjnych mających na celu wprowadzenie ustawowych podstaw prawnych dla przekazywania danych osobowych uczniów podmiotom prowadzącym działalność leczniczą w związku z realizacją umów w ramach profilaktycznej opieki zdrowotnej nad dziećmi i młodzieżą. Generalny Inspektor zauważył, że kwestia podstaw prawnych ww. przekazywania danych jest od dłuższego czasu przedmiotem wątpliwości i pytań kierowanych do organu ochrony danych osobowych, w szczególności przez dyrektorów szkół, którym przedstawiane były żądania przekazywania wykazu/baz uczniów lub młodzieży. Podmioty lecznicze występujące z takimi żądaniami w uzasadnieniu powoływały się na § 27 pkt. 6. 1 Zarządzenia Prezesa NFZ nr 74/2010/DSOZ z dnia 1 grudnia 2010 r. w sprawie określenia warunków zawierania i realizacji umów o udzielanie świadczeń w rodzaju: podstawowa opieka zdrowotna, zmienionym Zarządzeniem nr 87/2010/DSOZ z dnia 29 grudnia 2010 r. oraz w sposób ogólny – na rozporządzenie Ministra Zdrowia z dnia 29 sierpnia 2009 r. w sprawie wykazów świadczeń gwarantowanych z zakresu podstawowej opieki zdrowotnej (Dz. U. Nr 139, poz. 1139 z późn. zm.) i rozporządzenie Ministra Zdrowia z dnia 28 sierpnia 2009 r. w sprawie organizacji profilaktycznej opieki nad dziećmi i młodzieżą (Dz. U. Nr 139 poz. 1133). Jak zauważył Generalny Inspektor, wśród obowiązujących unormowań brakowało przepisu, który mógłby stanowić podstawę przekazywania przez dyrektorów szkół danych osobowych uczniów w celu wykonywania umów, których stronami są szkoły i świadczeniodawcy. Przypomniał także, że pismem z dnia 27 marca 2012 r. zwrócił się do Prezesa Narodowego Funduszu z prośbą o zajęcie stanowiska w przedmiotowej sprawie.

W odpowiedzi Prezes Narodowego Funduszu Zdrowia wskazał, że przyjęcie rozwiązań umożliwiających finansowanie ze środków publicznych świadczeń z wykorzystaniem sposobu opartego na kapitałowej stawce rocznej - dla jego przejrzystości oraz pełnej wiarygodności przekazywanych świadczeniodawcom środków finansowych - wymaga dokonywania weryfikacji danych podopiecznych (uczniów) placówek oświatowych. W obecnym stanie prawnym istnieją przepisy wykonawcze, na których oparto powyższe rozwiązania. Jednakże w opinii Prezesa NFZ zasadne jest rozważenie w tym zakresie przyjęcia jednoznacznych i bezspornych regulacji prawnych do przekazywania danych o uczniach szkół w celu właściwego wydatkowania środków publicznych przez Fundusz. Generalny Inspektor poinformował, że zgodnie z art. 51 ust. 5 Konstytucji Rzeczypospolitej Polskiej, zasady i tryb gromadzenia oraz udostępniania informacji powinna określać ustawa. W przekonaniu Generalnego Inspektora konieczne jest zatem, aby zasady i zakres udostępniania danych uczniów przez dyrektorów szkół świadczeniodawcom realizującym świadczenia z zakresu profilaktycznej opieki zdrowotnej nad dziećmi i młodzieżą, uregulowane zostały w przepisach rangi ustawowej. Rozporządzenie natomiast może jedynie konkretyzować regulacje ustawowe, nie zaś stanowić samoistną podstawę dla obowiązku lub uprawnienia do żądania przekazywania tych danych.

Generalny Inspektor zwrócił się o podjęcie prac legislacyjnych, deklarując jednocześnie chęć współpracy i udziału w tym procesie, jako że stosownie do art. 12 ustawy o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych ma nie tylko prawo, ale i obowiązek opiniować projekty aktów prawnych, jak również inicjować doskonalenie obecnie obowiązujących przepisów dotyczących ochrony danych osobowych. Poinformował przy tym, że niniejszą sprawę przedstawi również ministrowi właściwemu do spraw edukacji wnioskując o poparcie dla tej inicjatywy oraz wzięcie czynnego udziału w pracach legislacyjnych w tym zakresie.

## **7.2. Działalność informacyjna**

Do działalności informacyjnej GIODO, podobnie jak w latach ubiegłych, wykorzystywane były różnorodne kanały komunikacyjne, takie jak:

- strona internetowa,
- Infolinia,
- Newsletter,
- konferencje i seminaria naukowe,
- szkolenia,
- kampanie edukacyjne i informacyjne, m.in. takie jak Dzień Ochrony Danych Osobowych czy Dni Otwarte GIODO,
- publikacje książkowe,
- współpraca z mediami.

Dzięki ich wykorzystaniu możliwe było przekazanie szerokiemu gronu odbiorców, najistotniejszych informacji z zakresu ochrony danych osobowych oraz działalności Biura GIODO.

W celu upowszechniania wiedzy z zakresu ochrony danych osobowych, Generalny Inspektor w 2012 r., wzorem lat ubiegłych, korzystał z pośrednictwa mediów (prasa, radio, telewizja, agencje informacyjne i portale internetowe), organizując konferencje prasowe i kampanie informacyjne, udzielając wywiadów, odpowiadając na indywidualne pytania dziennikarzy, jak też przekazując – z własnej inicjatywy – te najistotniejsze informacje, które wymagały szybkiego nagłośnienia. Wykorzystywana była również w tym celu - będąca jednocześnie Biuletynem Informacji Publicznej - strona internetowa GIODO ([www.giodo.gov.pl](http://www.giodo.gov.pl)), która jest na bieżąco uzupełniana i aktualizowana.

Z kolei informacje do pojedynczych odbiorców trafiały zarówno w formie pism, jak i ustnych wyjaśnień udzielanych za pośrednictwem Infolinii oraz podczas indywidualnych spotkań interesantów z pracownikami Biura GIODO, w tym z zastępcą GIODO, w ramach dyżurów. Duży krąg odbiorców informacji z zakresu ochrony danych osobowych zapewniły również inicjowane przez GIODO szkolenia oraz konferencje naukowe oraz publikacje prasowe i książkowe.

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.

## **7.2.1. Współpraca ze środkami masowego przekazu**

### **1. Stałe kontakty z mediami**

Wzorem lat ubiegłych, w roku 2012 organ do spraw ochrony danych osobowych kontynuował stałą współpracę z mediami polegającą na przekazywaniu do publikacji opracowanych przez GIODO materiałów informacyjno-edukacyjnych. Taka współpraca była prowadzona zarówno z prasą codzienną o zasięgu ogólnopolskim, przede wszystkim z „Rzeczpospolitą” „Dziennikiem Gazetą Prawną” i „Pulsem Biznesu”, jak i ogólnopolskimi pismami branżowymi, m.in. „Serwisem Prawno-Pracowniczym”, „Przeglądem Komunalnym”, „Computerworldem”, „IT w Administracji” oraz portalami internetowymi, w tym będącymi odpowiednikami prasy drukowanej (jak np. Dziennik Internautów czy lex.pl). Upowszechnianiu wiedzy z zakresu ochrony danych osobowych służyła też publikacja wyjaśnień GIODO w czasopismach kobiecych, takich jak np. „Twoje Imperium” czy „Świat Kobiety”. W 2012 r. stała współpraca GIODO ze stacjami telewizyjnymi i radiowymi, m.in. z Informacyjną Agencją Radiową, Polskim Radiem Jedyneką, Radiem TOK FM, Radiem dla Ciebie, TVP INFO, Telewizją Polsat czy TVN24, zaowocowała regularnym upowszechnianiem w tych mediach problematyki z zakresu ochrony danych osobowych.

W 2012 r. w prasie, radiu, telewizji i Internecie opublikowanych lub wyemitowanych zostało około **160** 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.

Wśród problemów, o które najczęściej pytali przedstawiciele mediów, były m.in.:

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii, zwłaszcza modelu *cloud computing*,
- funkcjonowanie portali społecznościowych, w tym wykorzystywanie przez nie danych osobowych,

- 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, zwłaszcza ich upubliczniania,
- 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 przedsiębiorców, w kontekście zniesienia art. 7a ustawy Prawo działalności gospodarczej,
- upublicznianie przez jednostki samorządu terytorialnego danych osobowych w BIP, 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,
- pozyskiwanie danych osobowych przez organizatorów konkursów internetowych i SMS'owych,
- nagrywanie przez instytucje publiczne i firmy prywatne rozmów z klientami w kontekście przepisów o ochronie danych osobowych,
- przetwarzanie danych osobowych przez spółdzielnie i wspólnoty mieszkaniowe.

W 2012 r. GODO udzielił – pisemnie lub telefonicznie – około **290** takich odpowiedzi.

### **3. Wywiady i wystąpienia**

Tematyka wywiadów radiowych i telewizyjnych oraz udzielonych dziennikarzom prasy drukowanej i internetowej 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, a także ochrona danych osobowych w kontekście rozwoju nowoczesnych technologii. Dziennikarze pytali również o to, 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: wyludzanie bądź wykradanie danych osobowych, monitorowanie pracowników czy instalacja inteligentnych liczników energetycznych.

Zmiany w przepisach dotyczących funkcjonowania systemu informacji oświatowej oraz tworzenie systemu informacji w ochronie zdrowia, to kolejny temat częstych wystąpień medialnych GIODO w 2012 r. Duże zainteresowanie mediów budziła także reforma prawa regulującego ochronę danych osobowych na poziomie Unii Europejskiej, zarówno w kontekście zakresu planowanych zmian, jak i ich wpływu na prawodawstwo krajowe. Ponadto GIODO 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. W 2012 r. GIODO udzielił blisko **240** wywiadów.

#### a) **Konferencje prasowe**

W związku z potrzebą nagłośnienia niektórych wydarzeń lub upublicznienia stanowiska GIODO w istotnych dla ochrony danych osobowych sprawach, GIODO w 2012 r. zorganizował 8 konferencji prasowych. Poświęcone one były:

- obchodom VI Dnia Ochrony Danych Osobowych w Polsce i w Brukseli (30 stycznia 2012 r. w Warszawie oraz 24 stycznia 2012 r. w Brukseli),
- reformie unijnych przepisów dotyczących ochrony danych osobowych (7 marca 2012 r.),
- programowi edukacyjnemu GIODO „Twoje dane - Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli” w związku z uroczystą inauguracją trzeciej jego edycji. Omówione zostały podstawowe zasady ochrony danych osobowych w sektorze oświaty oraz uprawnienia i obowiązki dyrektora szkoły jako administratora danych osobowych, a także zaprezentowano metody edukowania dzieci i młodzieży z zakresu ochrony danych osobowych i prywatności (8 października 2012 r.),
- zjawisku kradzieży tożsamości i sposobom jego zapobiegania (11 października 2012 r.),
- zasadom przetwarzania danych osobowych przez podmioty z sektora motoryzacyjnego, w związku z podpisaniem przez GIODO i Polski Związek Przemysłu Motoryzacyjnego Kodeksu dobrych praktyk (16 listopada 2012 r.),
- nowej inicjatywie GIODO, jaką jest organizacja w różnych miejscach Polski, Dni Otwartych GIODO, podczas których odbywają się seminaria i szkolenia upowszechniające zasady ochrony danych osobowych, a także udzielane są bezpłatne porady prawne dla wszystkich zainteresowanych tą tematyką. Pierwsze Dni Otwarte GIODO odbyły się 22 listopada 2012 r. w Dąbrowie Górniczej i 23 listopada 2012 r. w Krakowie, a każde z tych wydarzeń poprzedziła konferencja prasowa. Podczas spotkań z dziennikarzami GIODO odnosił się zarówno do głównej tematyki Dni, jak i odpowiadał na pytania dotyczące interesujących dziennikarzy zagadnień związanych z ochroną danych osobowych i prawem do prywatności, m.in. takich, jak handel danymi osobowymi, upublicznianie danych osobowych przez urzędy administracji

publicznej czy zagrożenia, jakie dla ochrony danych osobowych i prywatności stanowi rozwój nowych technologii.

#### **b) Akcje informacyjno – promocyjne**

Do stałych akcji informacyjno-promocyjnych należy organizacja Dnia Ochrony Danych Osobowych, która w 2012 r. przeprowadzona została po raz szósty. W ramach VI Dnia Ochrony Danych Osobowych odbyło się w Brukseli spotkanie GIODO z eurodeputowanymi (24.01.2012 r.) zorganizowane we współpracy z europosem Jackiem Protasiewiczem, członkiem Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych PE, a także uroczysty wieczór w siedzibie Stałego Przedstawicielstwa Rzeczypospolitej Polskiej przy Unii Europejskiej z udziałem polskich posłów do Parlamentu Europejskiego, rzeczników ochrony danych osobowych z państw Unii Europejskiej, z Peterem Hustinxem, Europejskim Rzecznikiem Ochrony Danych Osobowych, przedstawicielami Komisji Europejskiej oraz innych polskich i unijnych instytucji mających siedzibę w Brukseli. Uroczystość zorganizowano we współpracy z polskim ambasadorem przy Unii Europejskiej, Panem Janem Tombińskim. W ramach obchodów VI Dnia Ochrony Danych Osobowych, 25 stycznia 2012 r. w Brukseli odbyła się międzynarodowa konferencja „Komputery, ochrona danych i prywatności”. podczas której GIODO wygłosił referat w sesji poświęconej ochronie danych i prywatności w inteligentnych systemach elektroenergetycznych.

Natomiast obchody VI Dnia Ochrony Danych Osobowych w Polsce, które przebiegały pod hasłem „Co Państwo wie o obywatelach? Zasady przetwarzania danych w rejestrach publicznych”, odbyły się 30 stycznia 2012 r. Tego dnia tradycyjnie zorganizowano Dzień Otwarty, na który złożyły się:

- konferencja „Co Państwo wie o obywatelach. Zasady przetwarzania danych w rejestrach publicznych” z udziałem przedstawicieli Trybunału Konstytucyjnego, Rzecznika Praw Obywatelskich, Ministerstwa Spraw Wewnętrznych i Administracji, Głównego Urzędu Statystycznego, Helsińskiej Fundacji Praw Człowieka, a także reprezentantów szkół wyższych i organizacji pozarządowych działających na rzecz bezpieczeństwa i praw obywateli w sieci,
- bezpłatne porady i konsultacje ekspertów z Biura GIODO,
- panel dyskusyjny „Co Państwo wie o obywatelach? Zasady przetwarzania danych w rejestrach publicznych” zorganizowany przez GIODO oraz redakcję „Dziennika Gazety Prawnej”, który odbył się 4 stycznia 2012 r. w siedzibie redakcji (publikacja jego zapisu miała miejsce 30 stycznia 2012 r.),
- wideoczat z GIODO zorganizowany w redakcji portalu Wirtualna Polska, który poświęcony był temu, co państwo wie o obywatelach, co powinno wiedzieć, a jakich informacji o nas nie powinno zbierać i wykorzystywać (31 stycznia 2012)

Informacje o wszystkich wymienionych wyżej wydarzeniach dotyczących Dnia Ochrony Danych Osobowych zaowocowały publikacją licznych artykułów prasowych i internetowych związanych z jego tematem przewodnim.

W 2012 r. GIODO po raz pierwszy włączył się do tzw. akcji wakacyjnej organizowanej przez Urząd Ochrony Konkurencji i Konsumentów pod hasłem „Przed wakacjami - co warto wiedzieć?”. Na jej potrzeby przygotowany został poradnik poświęcony temu, jak chronić dane osobowe w sytuacjach, jakie najczęściej mają miejsce podczas urlopów czy organizacji wakacyjnych wyjazdów. W przystępny sposób omówiono w nim m.in. zasady przetwarzania danych osobowych przez biura turystyczne, hotele i pensjonaty, przypomniano o bezprawności żądania pozostawiania dowodu osobistego w zastaw za wypożyczany sprzęt, a także wskazano, w jakich sytuacjach dopuszczalne jest kserowanie dowodu osobistego. Przypomniano także, by podczas wypełniania formularzy zwracać uwagę na zawarte w nich klauzule zgody na przetwarzanie danych osobowych, uważnie je przeczytać przed podpisaniem, by nie paść ofiarą nieuczciwych praktyk stosowanych przez firmy wyludzające dane osobowe. Poradnik został zamieszczony na stronie internetowej GIODO, a linki do niego znalazły się na stronach internetowych innych urzędów i instytucji biorących udział w tej akcji (w sumie ponad 30). Tematy poruszane w poradniku GIODO zostały podjęte przez większość mediów.

#### **4. Infolinia**

Ważną rolę w działalności informacyjnej Generalnego Inspektora Ochrony Danych Osobowych pełnił, działający w godzinach pracy, telefon informacyjny, tzw. Infolinia. W 2012 r. za jego pośrednictwem udzielono wyjaśnień ponad **11 tysiącom** osób.

#### **5. Newsletter**

W 2012 r. GIODO kontynuował wydawanie Newslettera, dostarczanego każdemu zainteresowanemu jego otrzymywaniem, poprzez zarejestrowanie się za pośrednictwem strony internetowej GIODO. W 2012 r. ukazało się **12** jego numerów.

### **7.2.2. Publikacje**

W 2012 r. ukazały się następujące publikacje Generalnego Inspektora Ochrony Danych Osobowych, w związku z jego udziałem w różnego rodzaju wydarzeniach organizowanych w kraju i za granicą:

- „15 lat ochrony danych w Polsce oraz w Europie Środkowej”, który został zawarty w publikacji pod red. włoskiego Organu Ochrony Danych "Le tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e bilanciamenti", a cura di Giuseppe Franco Ferrari, Milano, Egea, 2012.

W pracy tej Generalny Inspektor przybliżył kluczowe elementy historii powstawania prawa o ochronie danych w Polsce, strukturę Biura GIODO, sposób realizacji ustawowych zadań organu ds. ochrony



danych osobowych, a także nakreślił współpracę z organami ochrony danych z państw Europy Środkowo-Wschodniej.

- „Tworzenie profili osobowych w oparciu o ogólnie dostępne dane” (Personal Profiling Based on Generally Accessible Data), który został opublikowany w bułgarskim czasopiśmie „International Journal of Information Technologies & Security”.

Artykuł dotyczy kwestii istotnego zagrożenia związanego z wykorzystywaniem danych z różnych źródeł w działalności gospodarczej, wykorzystywaniem technik profilowania na potrzeby bieżącej i przyszłej oceny klientów (byłych, obecnych i potencjalnych), pracowników czy partnerów biznesowych. Główne pytanie postawione w artykule dotyczy tego, czy takie przetwarzanie może obejmować tworzenie profili osobowych, a jeżeli tak, to czy istnieją ograniczenia dla takich działań oraz środki prawne pozwalające na sprawowanie kontroli nad przetwarzaniem i na ograniczenie jego zakresu.

- “Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation. ENISA 2012”.

[http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/at\\_download/fullReport](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/at_download/fullReport)

- Cyber Europe was the biggest pan-European cyber security exercise to date. This report gives the key findings from ENISA, ENISA 2012.

[http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report/at\\_download/fullReport](http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report/at_download/fullReport)

- Grażyna Szpor, Wojciech R. Wiewiórowski (red.), „Internet. Prawno-informatyczne problemy sieci, portali i e-usług”. Warszawa 2012, Wyd. C.H. BECK.

### **7.2.3. Dni Otwarte Generalnego Inspektora Ochrony Danych Osobowych**

Dni Otwarte GIODO organizowane w różnych miejscach w Polsce to nowa inicjatywa Generalnego Inspektora Ochrony Danych Osobowych, będąca odpowiedzią na potrzeby edukacyjno-informacyjne zgłaszane przez wiele podmiotów zajmujących się ochroną danych osobowych. Przedsięwzięcie to ma umożliwić osobom zainteresowanym problematyką ochrony danych osobowych udział w specjalistycznych konferencjach, szkoleniach oraz dyskusjach, które z założenia odbywać się będą blisko ich miejsca zamieszkania. Pomysł Dni Otwartych GIODO jest nawiązaniem do cieszącego się dużym zainteresowaniem Dnia Otwartego w Biurze GIODO, który co roku organizowany jest w Warszawie w związku z obchodami Dnia Ochrony Danych Osobowych 28 stycznia.

#### **I Dzień Otwarty GIODO w Dąbrowie Górniczej**

Po raz pierwszy Dzień Otwarty GIODO odbył się 22 listopada 2012 r. w Dąbrowie Górniczej, a do uczestnictwa w nim zapraszał Generalny Inspektor Ochrony Danych Osobowych, Wyższa Szkoła

Biznesu w Dąbrowie Górniczej oraz Prezydent Miasta Dąbrowa Górnicza. Wybór tego miasta nie był przypadkowy. Od dawna GODO prowadzi współpracę z Wyższą Szkołą Biznesu w Dąbrowie Górniczej, zaś położenie miasta dodatkowo wpłynęło na wysoką frekwencję mieszkańców Górnego Śląska i Zagłębia.

Głównym celem I Dnia Otwartego GODO w Dąbrowie Górniczej było przeprowadzenie debaty na temat szeroko pojętej problematyki ochrony danych osobowych oraz prawa do prywatności, w tym planowanej unijnej reformy prawa w tym zakresie i jej konsekwencjach dla administratorów danych osobowych. Wydarzenie zostało podzielone na część konferencyjną oraz szkoleniową, co umożliwiło wymianę poglądów i doświadczeń pomiędzy przedstawicielami organu ds. ochrony danych osobowych a praktykami - reprezentantami instytucji społecznych, administracji publicznej, przedsiębiorców oraz z przedstawicielami świata nauki.

Na I Dzień Otwarty GODO złożyły się: Konferencja „Prawo nowych technologii w zakresie ochrony danych osobowych i prawa do prywatności” wraz z panelem dyskusyjnym dla przedsiębiorców pt. „Kontrola GODO w praktyce”, które odbyły się w siedzibie Wyższej Szkoły Biznesu w Dąbrowie Górniczej oraz szkolenie dla przedstawicieli administracji publicznej zorganizowane w siedzibie Urzędu Miasta. Podczas Konferencji dr Wojciech R. Wiewiórowski, GODO, wygłosił referat zatytułowany „Prawo do bycia zapomnianym. Podstawowe prawo człowieka czy groźba stworzenia Ministerstwa Prawdy?”

## **II Dzień Otwarty GODO w Krakowie**

Z myślą o mieszkańcach Małopolski, w dniu 23 listopada 2012 r. zorganizowany został w Krakowie II Dzień Otwarty GODO, którego współorganizatorami byli Uniwersytet Jagielloński i Instytut Allerhanda.

Głównym punktem II Dnia Otwartego GODO była konferencja naukowa poświęcona prawnym i informatycznym aspektom ochrony prywatności w świecie nowych technologii komunikacyjnych, która odbywała się w Sali Audytoryjnej Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego. Konferencję otworzył referat wygłoszony przez dra Wojciecha Rafała Wiewiórowskiego, Generalnego Inspektora Ochrony Danych Osobowych, poświęcony zagadnieniu oceny skutków przedsięwzięcia dla ochrony prywatności (Privacy Impact Assessment) – kluczowemu problemowi z punktu widzenia planowania przedsięwzięć, w ramach których może dochodzić do ingerencji w sferę prywatności innych osób.

Konferencja, którą poprzedziło spotkanie z mediami, cieszyła się dużym zainteresowaniem szerokiego kręgu odbiorców, zwłaszcza osób, które na co dzień zajmują się prawnymi i informatycznymi aspektami bezpieczeństwa informacji, tj. informatyków, prawników, administratorów bezpieczeństwa informacji, pracowników administracji publicznej i przedsiębiorców. Potwierdzali oni, że istnieje potrzeba organizacji tego typu wydarzeń, co utwierdziło GODO

w przekonaniu, że idea Dni Otwartych GIODO, odbywających się w różnych regionach Polski, powinna być kontynuowana.

#### 7.2.4. Szkolenia

##### **Szkolenia podmiotów zewnętrznych**

W ramach szeroko prowadzonej działalności edukacyjnej, Generalny Inspektor Ochrony Danych Osobowych organizował nieodpłatne **szkolenia** skierowane głównie do instytucji publicznych zgłaszających zainteresowanie problematyką z zakresu ochrony danych osobowych.

Wśród podmiotów, które w 2012 r. zwróciły się do GIODO z prośbą o przeprowadzenie szkolenia znalazły się: Fundacja Rozwoju Społeczeństwa Obywatelskiego, Stowarzyszenie „Miasta w Internecie” i Świętokrzyskie Partnerstwo dla Rozwoju Społeczeństwa Informacyjnego, Warszawskie Centrum Innowacji Edukacyjnych i Szkoleń, Krajowy Zarząd Gospodarki Wodnej, Centrum Rozwoju Zasobów Ludzkich, Najwyższa Izba Kontroli, Narodowe Centrum Badań i Rozwoju, Regionalna Wojskowa Pracownia Psychologiczna w Krakowie, Polska Organizacja Handlu i Dystrybucji, Agencja Restrukturyzacji i Modernizacji Rolnictwa, Agencja Rynku Rolnego, Bank Pocztowy, Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych, Spółdzielcza Kasa Oszczędnościowo - Kredytowa, Spółka Hays Poland, Centralny Zarząd Służby Więziennej, Centralna Biblioteka Wojskowa – pracownicy bibliotek wojskowych i ośrodków informacji naukowej, Ośrodek Rozwoju Polskiej Edukacji za Granicą, Biuro Rzecznika Praw Obywatelskich, a także szkoły wyższe: Uniwersytet Ekonomiczny w Poznaniu, Warszawski Uniwersytet Medyczny, Almamater Szkoła Wyższa oraz Akademia Obrony Narodowej.

Ponadto w szkoleniach przeprowadzonych przez GIODO w 2012 r. udział wzięły Urzędy Miasta: Sopot, Wrocław, Częstochowa oraz Dąbrowa Górnicza, a także Okręgowa Izba Radców Prawnych w Warszawie, Okręgowa Rada Adwokacka w Krakowie, Wojewódzki Urząd Pracy w Kielcach, Sądy Okręgowe: w Łomży, w Płocku i Włocławku, Krajowa Rada Sądownictwa, Kancelaria Sejmu i Kancelaria Senatu, oraz przedstawiciele służb mundurowych, jak Służba Wywiadu Wojskowego oraz Komenda Główna Straży Granicznej. Na liście przeszkolonych przez Generalnego Inspektora Ochrony Danych Osobowych pracowników ministerstw znalazły się Ministerstwa: Spraw Zagranicznych (Centrum Rozwoju Zawodowego), oraz Nauki i Szkolnictwa Wyższego i Finansów. Natomiast w szkoleniu zorganizowanym dla Narodowego Banku Polskiego brali też udział przedstawiciele banków centralnych krajów Europy Wschodniej i Południowo-Wschodniej, w których trwa aktualnie proces wdrażania europejskich regulacji dotyczących bezpieczeństwa teleinformatycznego i ochrony danych osobowych.

Niektóre szkolenia miały ogólnopolski zasięg, jak te zorganizowane dla Centrali Kasy Rolniczego Ubezpieczenia Społecznego oraz 16 Oddziałów Regionalnych KRUS z całej Polski, dla Zarządów Dróg Wojewódzkich, czy też dwa szkolenia dla uczestników ogólnopolskiego Programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”. Pierwsze z nich odbyło się w lutym 2012 r. z udziałem nowo powołanych dyrektorów warszawskich placówek szkolnych i przedszkoli, a także doradców i konsultantów ośrodków doskonalenia zawodowego nauczycieli z Rybnika, Konina, Sieradza, Wrocławia, Skierniewic i Gliwic, którzy zgłosili swój udział do tego programu oraz dla przedstawicieli Ośrodka Rozwoju Edukacji w Warszawie. Drugie zaś (październik 2012 r.) - adresowane było do przedstawicieli szkół i placówek doskonalenia zawodowego nauczycieli ze wszystkich województw w kraju.

Na uwagę zasługuje także szkolenie sektorowe przeprowadzone przez przedstawicieli GIODO dla sekretarzy gmin podkarpackich oraz dwa szkolenia dla przedstawicieli samorządu terytorialnego Dolnego Śląska zorganizowane przez Urząd Miasta Wrocławia, w którym uczestniczyło w sumie kilkaset osób.

W sumie w 2012 r. przeprowadzono **65 szkoleń** z zakresu ochrony danych osobowych dla podmiotów zewnętrznych. Ich pełny wykaz znajduje się w załączniku nr 5. Wśród nich znalazło się także dwudniowe szkolenie dla tłumaczy Dyrekcji Generalnej ds. Tłumaczeń Pisemnych Komisji Europejskiej w Luksemburgu. W szkoleniu z zakresu międzynarodowych i krajowych podstaw prawnych ochrony danych osobowych, ich wdrożenia do polskiego porządku prawnego oraz w warsztatach poświęconych terminologii, uczestniczyli zarówno tłumacze języka polskiego, jak i pozostałych unijnych języków.

W tym miejscu należy podkreślić, że wspomniany wykaz zawiera nie tylko szkolenia *sensu stricto*, ale obejmuje także spotkania, seminaria czy warsztaty o charakterze dydaktycznym czy popularnonaukowym, propagującym idee ochrony danych osobowych. Przykładem może być udział przedstawiciela GIODO w seminarium zorganizowanym przez Narodowy Bank Polski na temat europejskich regulacji prawnych w zakresie ochrony danych osobowych w kontekście bezpieczeństwa teleinformatycznego dla przedstawicieli banków centralnych krajów Europy Wschodniej i Południowo-Wschodniej, VIII Ogólnopolskie Forum Wojskowych Bibliotek i Ośrodków Informacji Naukowej, podczas którego przeprowadzone były zajęcia warsztatowe nt. nowelizacji ustawy o ochronie danych osobowych, czy też wspomniane szkolenie sekretarzy gmin, miast i powiatów województwa podkarpackiego, które odbyło się podczas konferencji. W konwencji szkolenia odbył się też wykład dla słuchaczy kierunków turystycznych i przedstawicieli hoteli indywidualnych i sieciowych wygłoszony przez przedstawiciela GIODO podczas seminarium na temat zagrożeń w procesie przetwarzania danych osobowych w branży hotelarskiej, oraz wideokonferencja nt. prawa do prywatności i ochrony

danych osobowych, zorganizowana dla prokuratorów w siedzibie Prokuratury Generalnej w Warszawie.

### **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 oraz praktykantów odbywających staże. 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.

Druga grupa szkoleń adresowana była głównie do pracowników sekretariatów, dyrektorów departamentów i pracowników zaangażowanych w proces obiegu dokumentów, w tym przygotowanie i wysyłanie odpowiedzi drogą elektroniczną przy wykorzystaniu systemów ESP-Doręczyciel i ePUAP.

Ponadto pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych uczestniczyli w dwudniowym szkoleniu pt. „Rodzina norm systemów zarządzania bezpieczeństwem informacji ISO/IEC 27000”.

### **Udział pracowników Biura GODO w szkoleniach organizowanych przez jednostki zewnętrzne**

Pracownicy Biura GODO korzystali ze szkoleń, warsztatów i seminariów 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. Wśród nich wymienić należy Forum koordynatorów czynności kancelaryjnych – „Instrukcja kancelaryjna po roku doświadczenia i dobre praktyki”, zorganizowane przez Centrum Promocji Informatyki (29.03.2012), Warsztaty Human Morion Analysis Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych w Warszawie (8.05.2012), Konferencja szkoleniowa PIIT „Oprogramowanie standardowe i systemy zamawiane” (29.05.2012), Warsztaty Urzędu Regulacji Energetyki dotyczące wdrażania Infrastruktury Sieci Domowej współpracującej z inteligentnymi sieciami (22.06.2012 i 11.09.2012), szkolenie z zakresu „Rodzina norm systemów zarządzania bezpieczeństwem informacji ISO/IEC 27000” (26-29.06.2012), szacowania i oceny ryzyka (11.09.2012), Warsztaty SECURE Hands-on pt. „Wykrywanie i analiza ataków sieciowych” (22-24.10.2012), konferencje szkoleniowe: Check Point Security Day 2012 (20.09.2012), „Motor Control

Conference” na Akademii Wychowania Fizycznego w Katowicach (27.09-2.10.2012) oraz seminarium szkoleniowe „Rozwiązania Check Point w sektorze publicznym” (29-30.11.2012).

W dniu 20 listopada 2012 r. pracownicy Biura GODO brali udział w XII Forum Administratorów, Koordynatorów i Redaktorów BIP, podczas którego odbyło się szkolenie z zagadnień związanych z funkcjonowaniem tego trybu udostępniania informacji, ochrony danych osobowych i zasad anonimizacji udostępnianych treści, teorii i praktyki ponownego wykorzystywania informacji publicznej, ograniczenia w dostępie do informacji publicznej oraz problemy prawne wynikające z prowadzenia BIP. Organizatorem szkolenia było Centrum Promocji Informatyki.

Ponadto pracownicy Biura uczestniczyli w organizowanym cyklicznie szkoleniu z zasad Bezpieczeństwa i Higieny Pracy.

### **7.2.5. Konkursy**

W analizowanym 2012 r. Generalny Inspektor Ochrony Danych Osobowych był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

**I. „Ochrona danych osobowych kandydatów do pracy przetwarzanych w sieci informatycznej”** – to tytuł 2. edycji konkursu wiedzy o ochronie danych osobowych dla studentów wydziałów prawa szkół wyższych, zorganizowanego przez Generalnego Inspektora Ochrony Danych Osobowych przy wsparciu merytorycznym PricewaterhouseCoopers Legal Szurmińska-Jaworska Sp. K. 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 13 prac. Zwycięzcy konkursu otrzymali nagrody w postaci tabletów PC oraz możliwość odbycia praktyk zawodowych w Biurze GODO. Uroczyste wręczenie nagród odbyło się w dniu 29 maja 2012 r. na Uczelni Kardynała Stefana Wyszyńskiego w Warszawie podczas IV Konferencji Naukowej „Bezpieczeństwo w Internecie: cloud computing – przetwarzanie w chmurze”.

#### **II. Druga edycja konkursu dla sklepów internetowych „Bezpieczny eSklep 2012”**

Celem konkursu „Bezpieczny eSklep” było wyróżnienie najbardziej wiarygodnych i rzetelnych sklepów internetowych w Polsce i tym samym podniesienie jakości i poziomu usług handlu elektronicznego. Organizatorem Konkursu był Instytut Logistyki i Magazynowania z Poznania. Konkurs objęty został honorowym patronatem Ministra Gospodarki oraz Generalnego Inspektora Ochrony Danych Osobowych. W konkursie „Bezpieczny eSklep” ocena sklepów przebiegała w dwóch etapach. W pierwszym etapie pod uwagę brane były trzy czynniki: poprawność formalna oraz prawna w zakresie zastosowanych zapisów regulaminowych, sposobu obsługi koszyka zamówień oraz zgodność z prawem ochrony danych osobowych. W drugim etapie Kapituła Konkursu - w której

zasiadał Minister Andrzej Lewiński, Zastępca Generalnego Inspektora Ochrony Danych Osobowych - oceniała sklepy m.in. w zakresie czytelności strony internetowej, opisów oferowanych towarów, przejrzystości regulaminu sklepu i stosowania zasad dobrych praktyk gospodarczych.

## 7.2.6. Projekty i programy

W roku sprawozdawczym 2012, 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 latach 2012-13 Biuro GIODO będzie realizowało III edycję projektu mobilności finansowanego z środków Unii Europejskiej w ramach Programu Leonardo da Vinci będącego częścią ww. Programu „Uczenia się przez całe życie”. Dotychczas Biuro GIODO zrealizowało dwa projekty mobilności w ramach wymiany doświadczeń: w 2007 r. (pt. Nowe kompetencje osób odpowiedzialnych za wykonywanie przepisów ochrony danych osobowych) i w 2009 r. (Wzmocnienie umiejętności pracowników Biura GIODO). Celem nowego projektu jest umożliwienie pracownikom Biura GIODO wymiany wiedzy i doświadczeń w zakresie stosowania prawa o ochronie danych osobowych z innymi instytucjami europejskimi zajmującymi się szeroko rozumianą ochroną praw człowieka oraz organami ochrony danych w krajach Unii Europejskiej, poprzez odbycie stażu: w Departamencie Ochrony Danych i Cyberprzestępstw Dyrekcji Generalnej Praw Człowieka i Spraw Prawnych Rady Europy, u Europejskiego Rzecznika Ochrony Danych w Belgii (the European Data Protection Supervisor - EDPS), w Akademii Prawa Europejskiego w Niemczech (the Academy of European Law), Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji w Grecji (the European Network and Information Security Agency - ENISA), w biurze Bułgarskiej Komisji ds. Ochrony Danych Osobowych (Commission for Personal Data Protection) oraz w biurze Chorwackiej Agencji Ochrony Danych Osobowych (Croatian Personal Data Protection Agency). Uczestnicy zostali aktywnie zaangażowani w zadania i prace przydzielone im przez instytucje partnerów, np. w przygotowanie konferencji międzynarodowej, w ENISA zostali włączeni do realizacji projektu badawczego, w Biurze EDPS pracowali nad zagadnieniami związanymi z tworzeniem i egzekwowaniem prawa ochrony danych na szczeblu krajów UE, w siedzibie Rady Europy oraz w organach ochrony danych Chorwacji i Bułgarii byli włączeni do codziennych prac tych urzędów. Szczegółowy program pobytu był

dopasowany do indywidualnych potrzeb każdego uczestnika wyjazdu i odpowiadał charakterowi pracy wykonywanemu w polskim urzędzie ochrony danych osobowych. W trakcie staży uczestnicy zostali zaangażowani do codziennych prac realizowanych w ramach poszczególnych organizacji, uczestniczyli w opracowywaniu różnych dokumentów i raportów w zakresie ochrony danych, w realizacji międzynarodowych projektów badawczych, w spotkaniach, konferencjach, warsztatach organizowanych przez instytucje partnerów, a także realizowali zadania związane ze wzmocnieniem bezpieczeństwa IT, w czynnościach kontrolnych oraz innych zadaniach wyznaczonych przez partnera.

Projekt zakładał udział pracowników Biura GIODO w stażach trwających od 2 tygodni do 4 miesięcy. W rezultacie projektu uczestnicy poznali standardy pracy oraz zakres zadań realizowanych w poszczególnych instytucjach partnerów, a także mieli szansę wdrożenia się do pracy w instytucjach międzynarodowych. Ponadto udział w projekcie przyczynił się do wzrostu mobilności zawodowej pracowników Biura GIODO. Projekt realizowany będzie w terminie od 1 czerwca 2012 r. do 30 grudnia 2013 r.

**b)** W 2012 r. Biuro GIODO rozpoczęło realizację kolejnego projektu partnerskiego finansowanego ze środków Unii Europejskiej w ramach Programu Leonardo da Vinci będącego częścią Programu „Uczenia się przez całe życie” (*Lifelong Learning Programme*) pt. „Zwiększanie świadomości w zakresie ochrony danych wśród pracowników zatrudnionych w krajach Unii Europejskiej” (Raising awareness of the data protection issues among the employees working in the EU”). Projekt realizowany będzie w latach 2012-2014 we współpracy z Chorwacką Agencją Ochrony Danych Osobowych, Czeskim Urzędem Ochrony Danych oraz Bułgarską Komisją Ochrony Danych Osobowych. Zasadniczym celem projektu jest przygotowanie materiałów edukacyjnych skierowanych do osób fizycznych podejmujących zatrudnienie lub pracujących w jednym z krajów uczestniczących w projekcie. Doświadczenia płynące ze wszystkich krajów partnerskich wskazały na brak kompleksowych informacji na temat zagadnień związanych z ochroną danych osobowych stosowanych w różnych obszarach życia. Brak usystematyzowanej wiedzy w tym obszarze został wskazany zarówno przez jednostki reprezentujące różne sektory działalności gospodarczej i publicznej, jak i pracowników (osoby fizyczne). W związku z tym konieczne jest podejmowanie wszelkich działań zmierzających do upowszechniania wiedzy na temat ochrony danych osobowych i prywatności adresowanej do różnych grup odbiorców.

Inspirującym przy przygotowaniu tego projektu był pozytywny odbiór publikacji „Wybrane zagadnienia z zakresu ochrony danych. Przewodnik dla przedsiębiorców” przygotowanej w ramach projektu partnerskiego LdV, która ukazała się w 2011 r. Pozytywne opinie pochodzące od różnych grup odbiorców, głównie przedsiębiorców oraz przedstawicieli sektora biznesu i edukacji, ugruntowały przekonanie o potrzebie opracowania kolejnego przewodnika, tym razem skierowanego do pracowników podejmujących zatrudnienie w jednym z krajów uczestniczących w projekcie. Publikacja



przygotowana w ramach projektu skoncentrowana będzie na dostarczeniu tym osobom porad i wskazówek na temat wybranych zagadnień z zakresu ochrony danych osobowych i prywatności. Dzięki informacjom zawartym w przewodniku pracownicy uzyskają wiedzę na temat swoich praw i obowiązków w zakresie ochrony danych osobowych potrzebną do pracy i w codziennym życiu (np. w obszarze ubezpieczeń społecznych, zatrudnienia, działań marketingowych itp.) przed rozpoczęciem pracy w innym kraju.

W rezultacie projekt ukierunkowany będzie na upowszechnianie wiedzy w zakresie ochrony danych osobowych w sposób umożliwiający efektywną i samodzielną naukę przez bezpośrednich adresatów przepisów prawa w tym obszarze w krajach partnerskich i przyczyni się do wzmocnienia współpracy między europejskimi organami ochrony danych osobowych biorącymi w nim udział.

W tym miejscu podkreślenia wymaga, że w ramach przedstawionego projektu mobilności Leonardo da Vinci, z pięciodniową wizytą gościła w Biurze GIODO delegacja 5 przedstawicieli Bułgarskiej Komisji ds. Ochrony Danych Osobowych. Celem wizyty było umożliwienie przedstawicielom bułgarskiego i polskiego organu ochrony danych osobowych wymiany wiedzy i doświadczeń związanych z wdrażaniem prawa ochrony danych osobowych w tych dwóch krajach.

c) Biuro GIODO kontynuowało realizację rozpoczętego w 2010 r. 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 był w latach 2010-2012 we współpracy z Węgierskim Organem Ochrony Danych oraz Chorwacką Agencją Ochrony Danych Osobowych. Założeniem projektu było przeprowadzenie badań w Polsce, Chorwacji i na Węgrzech wśród dzieci i młodzieży, na temat ich podejścia do zagadnień związanych z ochroną danych osobowych i prywatności. Realizacja projektu miała umożliwić diagnozę poziomu świadomości dzieci i młodzieży na temat prawa do prywatności i ochrony danych osobowych, upowszechnienie wyników badań na poziomie krajowym i międzynarodowym – w szczególności zaś – ich porównanie między krajami biorącymi udział w projekcie, przygotowanie odpowiednich rekomendacji, a także zintensyfikowanie współpracy między organami ochrony danych w krajach członkowskich UE. Wiedza pozyskana w toku realizacji projektu przyczynić się miała do lepszego ukierunkowania działań informacyjnych w kraju i na świecie w kwestii sposobów ochrony danych osobowych i prywatności dzieci i młodzieży. Realizacja tego projektu została jednak przerwana w 2012 r.

W związku z dynamicznym rozwojem teleinformatyki i powszechnym korzystaniu przez dzieci i młodzież z tysięcy aplikacji oraz usług internetowych, GIODO podjął decyzję o kontynuacji badań w celu poznania podejścia najmłodszych użytkowników sieci do zagadnień związanych z ochroną danych osobowych i prywatności.

Badanie w formie ankiet rozesłane zostało do 120 szkół podstawowych i 120 gimnazjów wyselekcjonowanych losowo spośród wszystkich szkół w Polsce, a jego adresatami byli uczniowie klas piątych szkół podstawowych oraz gimnazjaliści klas trzecich. W rezultacie w badaniu udział wzięło 940 dzieci reprezentujących obie grupy wiekowe.

Z analizy wyników badań GIODO wynika, że dzieci i młodzież - niezależnie od tego, z jakich internetowych usług czy aplikacji korzystają - chętnie udostępniają swoje dane: imiona, nazwiska, adresy mailowe, wiek lub datę urodzenia, a także informacje dotyczące zainteresowań oraz swoje zdjęcia i filmy video. Uczniowie byli najbardziej skłonni udostępniać swoje dane osobowe w przypadku korzystania z portali społecznościowych, wysyłania e-maili czy komunikatorów internetowych, natomiast rzadziej upubliczniali swoje dane w przypadku chat-roomów, różnych forów czy blogów internetowych. Najczęściej dzieci i młodzież korzystają z Internetu w swoim domu (874 dzieci, co daje prawie 93% badanych osób), w szkole (ponad 55%) oraz w domu przyjaciół (ponad 32%). Dane pokazują, że już prawie co trzecie dziecko korzysta z Internetu w telefonie komórkowym. Dzieci i młodzież korzystają z Internetu głównie dla rozrywki – 796 dzieci, tj. prawie 85%, wskazało możliwość słuchania muzyki, oglądania filmów czy gier *on-line* jako jeden z celów korzystania z Internetu. Jednocześnie nieco mniej osób (prawie 74%) wykorzystuje Internet w celach edukacyjnych i poszukiwania informacji (np. materiałów do szkoły) oraz w celu nawiązywania i podtrzymywania kontaktów towarzyskich i utrzymywania relacji społecznych (np. poprzez korzystanie z portali społecznościowych itp.) – ponad 60%. Należy podkreślić, że Internet staje się również coraz częściej miejscem dokonywania zakupów przez dzieci i młodzież. Ponad 30% badanych wskazało na ten sposób dokonywania zakupów. Respondenci pytani też byli o to, ile średnio godzin dziennie spędzają przy komputerze korzystając z poszczególnych usług, serwisów czy aplikacji internetowych. Z odpowiedzi wynikało, że największą popularnością cieszą się portale społecznościowe, wyszukiwarki internetowe, e-maile, komunikatory internetowe czy gry *on-line*, z których do 3 godzin dziennie korzysta między 55-85% badanych dzieci. Z drugiej strony ponad 70% dzieci i młodzieży uczestniczących w badaniu w ogóle nie korzysta z chat-roomów, blogów czy stron komercyjnych.

Analiza zaprezentowanych wyników wskazuje na wagę zagadnień związanych z ochroną danych osobowych i prywatności przez dzieci i młodzież. Intensywne korzystanie z Internetu świadczy o jego dużej popularności wśród tej grupy odbiorców i dlatego należy zwracać szczególną uwagę na problem konieczności udostępniania danych osobowych oraz niezbędny zakres informacji ujawnianych podczas korzystania z Internetu. Wiedza pozyskana z realizacji tego badania umożliwi w przyszłości lepsze ukierunkowanie działań edukacyjno-informacyjnych GIODO, rodziców i opiekunów dzieci oraz podmiotów reprezentujących sektor edukacyjny i szkoleniowy, na temat sposobów ochrony danych osobowych i prywatności dzieci i młodzieży.

## II. Krajowy program edukacyjny

W 2012 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 w kolejnym roku szkolnym, ale także o rozszerzeniu obszaru działań tego programu na szkoły podstawowe i ponadgimnazjalne. W rezultacie do programu zgłosiło się 207 placówek z 16 województw - szkoły podstawowe, gimnazja, szkoły ponadgimnazjalne i placówki doskonalenia zawodowego nauczycieli, natomiast szkoły ponadgimnazjalne przystąpiły do niego na zasadzie pilotażu. Partnerami programu, z którymi zawarte zostały porozumienia o współpracy zostali: Gliwicki Ośrodek Metodyczny w Gliwicach, Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie oraz Śląska Sieć Metropolitarna Sp. z o.o.

W 2012 r. zostały zmienione zasady przystąpienia do programu. Szkoły i placówki doskonalenia zawodowego nauczycieli z całej Polski mogły się rejestrować za pomocą elektronicznego formularza bezpośrednio w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

Uroczysta inauguracja programu w roku szkolnym 2012/2013 odbyła się 8 października 2012 roku, konferencją zorganizowaną w Centralnej Bibliotece Rolniczej w Warszawie. Konferencja „Twoje dane – twoja sprawa, prawo do prywatności i ochrony danych osobowych we współczesnej szkole” była poświęcona szerokiemu spektrum zagadnień związanych z ochroną danych osobowych i prawem do

prywatności w ramach podejmowanych działań edukacyjnych i stanowiła kluczowe wydarzenie inaugurujące III edycję Ogólnopolskiego Programu Edukacyjnego Generalnego Inspektora Ochrony Danych Osobowych „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”. W czasie trwania części plenarnej konferencji zaprezentowano główne założenia i idee programu oraz wygłoszone zostały wykłady ekspertów zajmujących się ochroną danych osobowych oraz edukacją dzieci i młodzieży.

Podnoszenie wiedzy w zakresie ochrony danych osobowych i prawa do prywatności - zarówno wśród nauczycieli, jak i uczniów wydaje się szczególnie istotne w dobie globalizacji i szybkiego rozwoju nowych technologii. Edukacja dzieci i młodzieży w zakresie przysługujących im praw i nabywanie umiejętności skutecznego korzystania z nich, wydaje się szczególnym wyzwaniem dla ówczesnej edukacji.

Istotnym warunkiem uczestnictwa w programie był udział w szkoleniu na temat ochrony danych osobowych. Dwudniowe szkolenie dla uczestników programu zostało zorganizowane przez Generalnego Inspektora Ochrony Danych Osobowych w dniach 25-26 października 2012 r. w Warszawie.

Szkolenie było okazją do nabycia wiedzy na temat ochrony danych osobowych oraz umiejętności praktycznych w ramach przeprowadzonych z uczniami lekcji. W pierwszym dniu szkolenia zostały omówione zagadnienia związane z ochroną danych osobowych w szkołach. Uczestnicy nabyli podstawową i kompleksową wiedzę na temat genezy ochrony danych osobowych, zasad przetwarzania danych osobowych w placówkach oświatowych, rejestracji zbiorów danych osobowych oraz uzyskali praktyczne wskazówki będące wynikiem przeprowadzonych przez GODO kontroli. Natomiast drugi dzień szkolenia miał charakter warsztatowy. Był okazją do wymiany doświadczeń oraz poglądów z prekursorami Programu „Twoje dane- twoja sprawa...” na temat realizacji programu i prowadzenia zajęć o ochronie danych osobowych i prawie do prywatności. Uczestnikom szkolenia zaprezentowane zostały przykładowe lekcje dla uczniów oraz przekazane materiały edukacyjne wraz z płytą CD zawierającą scenariusze lekcji.

### **7.2.7. Konferencje, seminaria, spotkania**

W roku sprawozdawczym 2012, 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 różnych wydarzeniach, w tym również w organizowanych cyklicznie, jak chociażby obchody Światowego Dnia Społeczeństwa Informacyjnego w Polsce w 2012 r., który dotyczył zagadnień kultury w cyfrowym świecie, czy działaniom mającym długofalowy przebieg, jak akcja „Nie kopiuj głupoty” adresowana do

najmłodszych użytkowników sieci przez portal [nasza-klasa.pl](http://nasza-klasa.pl). Współpracował z organizacjami pozarządowymi i studenckimi poradniami prawnymi, zaś z Europejskim Stowarzyszeniem Studentów Prawa ELSA Poland współdziałał w związku z organizacją XIII Prawniczych Targów Pracy oraz Prawniczych Targów On – Line.

Na uwagę zasługuje nowa inicjatywa Generalnego Inspektora Ochrony Danych Osobowych organizowania konferencji, konsultacji, porad prawnych w ramach Dni Otwartych GIODO w wybranych miejscowościach całej Polski. Dotychczas odbyły się dwa tego rodzaju przedsięwzięcia – w Dąbrowie Górniczej i Krakowie.

Wykaz patronatów Generalnego Inspektora Ochrony Danych Osobowych udzielonych różnych wydarzeniom zorganizowanym w 2012 r. znajdują się w załączniku nr 6.

Poniżej przedstawione zostały najważniejsze wydarzenia krajowe o charakterze ogólnopolskim lub międzynarodowym z udziałem Generalnego Inspektora bądź przedstawicieli jego Biura. Ich pełny wykaz zawiera załącznik nr 7.

**1. Konferencja naukowa „Aktualne problemy dostępu do informacji publicznej” (Warszawa, 11 stycznia 2012 r.)**

Podczas Konferencji omawiane były zasady dostępu do informacji publicznej i jej ponownego wykorzystywania, a także kwestie związane z praktyką udostępniania informacji publicznej, w tym przez administrację publiczną, sądy administracyjne, szkoły wyższe. Osobny blok poświęcony był perspektywom zmian regulacji prawnych w tym zakresie. Konferencję zorganizował Wydział Prawa i Administracji UKSW oraz Naukowe Centrum Prawno - Informatyczne. Honorowy patronat nad tym wydarzeniem objęli: Prezes Naczelnego Sądu Administracyjnego, Rzecznik Praw Obywatelskich oraz Generalny Inspektor Ochrony Danych Osobowych.

**2. Obchody Dnia Ochrony Informacji Niejawnych (Siemianowice Śląskie, 20 stycznia 2012 r.)**

W 2012 roku po raz pierwszy zorganizowane zostały obchody Dnia Ochrony Informacji Niejawnych, których inicjatorem było Krajowe Stowarzyszenie Ochrony Informacji Niejawnych (KSOIN). Podczas obchodów tego święta, połączonego z Dniem Otwartym nt. ochrony informacji, przedstawione zostały zagadnienia wynikające ze współpracy Administratorów Bezpieczeństwa Informacji (ABI) z Pełnomocnikami Ochrony Informacji Niejawnych (POIN) w zakresie ochrony danych osobowych i informacji niejawnych – doświadczenia, uwagi i perspektywy funkcjonalne. Organizatorami obchodów tego wydarzenia byli: KSOIN oraz Wojskowe Zakłady Mechaniczne S.A.

**3. VI Dzień Ochrony Danych Osobowych – 28 stycznia 2012 r.**

W dniu 28 stycznia 2012 r. Generalny Inspektor Ochrony Danych Osobowych już po raz szósty 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 VI Dniem Ochrony Danych Osobowych odbywały się zarówno w Brukseli, jak i we wszystkich stolicach państw członkowskich Unii Europejskiej.

Z tej okazji 30 stycznia 2012 r. zorganizowany został w Biurze GIODO Dzień Otwarty, w ramach którego uczestnicy mieli okazję uzyskać informacje na temat ochrony danych osobowych, porady prawne i konsultacje. W tym dniu odbyła się także konferencja pod hasłem „Co Państwo wie o obywatelach? Zasady przetwarzania danych w rejestrach publicznych”. Konferencja podzielona została na trzy sesje tematyczne. Pierwsza z nich dotyczyła autonomii informacyjnej jednostki w kontekście działań władzy publicznej, druga – obejmowała kwestie związane z procesem tworzenia i zasadami funkcjonowania rejestrów publicznych, jako kluczowego zasobu infrastruktury informacyjnej państwa. Tematem kolejnej sesji było prawo do kontroli przetwarzania i dostępu do danych oraz mechanizmy nadzoru. Konferencję podsumował przewodniczący sesji trzeciej, dr Wojciech R. Wiewiórowski, GIODO, który w wystąpieniu pt. „Dane w rejestrach publicznych jako szczególna forma informacji sektora publicznego. Teoretycznoprawne uwarunkowania przetwarzania danych” podkreślił, że dane osobowe zawarte w rejestrach publicznych wymagają szczególnej ochrony i adekwatnych regulacji prawnych.

Obchodom VI Dnia Ochrony Danych Osobowych towarzyszyły również inne przedsięwzięcia, jak np. chat z Generalnym Inspektorem Ochrony Danych Osobowych w redakcji Wirtualnej Polski, podczas którego GIODO zaprosił wszystkich obywateli do dyskusji o tym, co Państwo wie o swoich obywatelach, co powinno wiedzieć, a czego nie powinno, a także uliczna gra miejska „Na tacy poDANE”, czy konferencje prasowe.

W ulicznej grze miejskiej „Na tacy poDANE” udział wzięły szkoły uczestniczące w ogólnopolskim Programie edukacyjnym „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli”. Organizatorem gry miejskiej był Gliwicki Ośrodek Metodyczny w Gliwicach wraz z Filią Gliwickiego Centrum Organizacji Pozarządowych „Dom Aktywnej Młodzieży”. W grze, która polegała na odnalezieniu określonych punktów kontrolnych w przestrzeni miejskiej i rozwiązaniu zadań dotyczących tematyki ochrony danych osobowych, uczestniczyło 10 gliwickich szkół.

Tradycyjnie Dzień Ochrony Danych Osobowych obchodzony był również w Brukseli, gdzie dr Wojciech Rafał Wiewiórowski, GIODO, spotkał się z posłami do Parlamentu Europejskiego, wziął udział w 5. Międzynarodowej Konferencji „Computers, Privacy and Data Protection”, a także zorganizował uroczyste spotkanie ekspertów ochrony danych osobowych w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej przy Unii Europejskiej.

#### **4. Konferencja „Szkoła Bezpiecznego Internetu” (Warszawa, 6 lutego 2012 r.)**

Organizatorami konferencji pt. „Szkoła Bezpiecznego Internetu” była Fundacja Kidprotect.pl oraz Wyższa Szkoła Nauk Społecznych PEDAGOGIUM w Warszawie. GODO przedstawił prezentację pt. „Ochrona prywatności małoletnich w sieci. Dlaczego rozwiązań prawnych z ‘realu’ nie da się zastosować do ‘wirtualu’?”. Podczas konferencji prezentowano wyniki badań dotyczące zachowań dzieci i młodzieży w sieci, a także podkreślono konieczność budowania świadomości odnośnie bezpiecznych zachowań w Internecie, zaznaczając rolę policji w tym zakresie. Podczas wydarzenia zostały wręczone wyróżnienia trzem szkołom, najbardziej aktywnym w ramach programu „Szkoła Bezpiecznego Internetu”.

**5. Konferencja „Cloud computing – z biznesem w chmurze” (Warszawa, 8 lutego 2012 r.)**

Zagadnienia prawne związane m.in. z bezpieczeństwem, ochroną danych osobowych, warunkami stosowania rozwiązań w chmurze w sektorze bankowym, zostały poruszone przez Generalnego Inspektora Ochrony Danych Osobowych w wystąpieniu pt. „Ochrona danych osobowych i tajemnic prawnie chronionych w chmurach obliczeniowych”. Organizatorem Konferencji była Firma MultiTrain.

**6. V Konferencja o bezpieczeństwie, audycie i zarządzaniu IT (Warszawa, 23 lutego 2012 r.)**

SEMAFOR 2012 to już piąta konferencja współorganizowana przez Computerworld, ISSA Polska (Information System Security Association) oraz ISACA Warsaw Chapter. Konferencja w całości poświęcona była zagadnieniom z obszaru zarządzania bezpieczeństwem informacji, audytu systemów informatycznych, zarządzania ryzykiem i nadzoru IT. Wystąpienie otwierające „Rola prawa stanowionego oraz standardów technicznych w tworzeniu zasad ochrony systemów teleinformatycznych” wygłosił Generalny Inspektor Ochrony Danych Osobowych.

**7. Konferencja „Kształcenie e-administracji” (Warszawa, 1 marca 2012 r.)**

Konferencja, której organizatorem był Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, Katedra Prawa Informatycznego, stanowiła forum wymiany informacji w kwestii aktualnego stanu edukacji dla e-administracji w Polsce oraz opinii dyrektorów generalnych urzędów różnych resortów na temat postulowanych zmian. Generalny Inspektor Ochrony Danych Osobowych wygłosił wystąpienie wprowadzające do sesji poświęconej służbie publicznej w społeczeństwie informacyjnym.

**8. Konferencja „Reforma regulacji ochrony danych osobowych w Unii Europejskiej. Wstępna ocena jej zakresu i konsekwencji (Warszawa, 7 marca 2012 r.)**

Konferencja, której organizatorami byli Generalny Inspektor Ochrony Danych Osobowych oraz Komisja Europejska, odbyła się w Krajowej Szkole Administracji Publicznej (KSAP). Wydarzenie było okazją do rozpoczęcia szerokiej dyskusji poświęconej planom ukształtowania nowego modelu ochrony prywatności i danych osobowych w Unii Europejskiej. Omówiono wybrane aspekty projektowanej reformy unijnych przepisów, jak: prawa osób, których dane dotyczą, konieczność

informowania o wycieku danych, nowa rola organów do spraw ochrony danych osobowych czy zmiany w podejściu do międzynarodowego transferu danych. W sesji poświęconej wybranym aspektom planowanych regulacji, referat pt. „Nowe europejskie regulacje w zakresie prywatności w fazie projektowania i prywatności” wygłosił Generalny Inspektor Ochrony Danych Osobowych.

**9. Konferencja „Przetwarzanie danych osobowych przedsiębiorców”** (Warszawa, 13 marca 2012)  
Omówieniu kwestii przetwarzania danych osobowych przedsiębiorców w związku z nowelizacją Prawa działalności gospodarczej, poświęcona była konferencja z udziałem Generalnego Inspektora Ochrony Danych Osobowych. Zaprezentowany został zakres stosowania ustawy o ochronie danych osobowych w odniesieniu do danych przedsiębiorców oraz kwestie związane ze zmianami w dokumentacji przetwarzania danych osobowych. Organizatorami konferencji byli Stowarzyszenie Administratorów Bezpieczeństwa Informacji (ABI) oraz firma European Network Security Institute (ENSI).

**10. Konferencja nt. planowanych zmian w prawodawstwie europejskim dotyczącym ochrony danych osobowych** (Wrocław, 20 marca 2012 r.)

Projektowaną unijną reformę prawa o ochronie danych zaprezentowano jako pochodną ryzyka związanego z rozwojem technologii informacyjnych. Omówiono także zagadnienia dostępu do informacji publicznej, w szczególności zaś kwestię zgody, jako istotnej przesłanki uprawniającej dany podmiot do przetwarzania danych osobowych w konkretnych sytuacjach, np. podczas rekrutacji. „Prawo do prywatności w świecie nowych technologii informacyjnych. Po co reformujemy unijne prawo ochrony danych” to tytuł wystąpienia Generalnego Inspektora Ochrony Danych Osobowych podczas tego wydarzenia. Konferencję zorganizował Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

**11. Okrągły Stół Generalnego Inspektora Ochrony Danych Osobowych ze środowiskiem prawniczym** (Warszawa, 29 marca 2012 r.)

Obecny stan polskich uregulowań z zakresu ochrony danych osobowych w kontekście projektowanych zmian prawa o ochronie danych w UE oraz propozycja nowelizacji obowiązującej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, której projekt jest przygotowywany przez GIODO celem przedłożenia władzy ustawodawczej, to tylko jeden z wielu tematów poruszanych podczas Okrągłego Stołu GIODO z podmiotami sektora prawniczego. Przedstawiciele GIODO omówili m.in. takie kwestie jak: rejestracja zbiorów danych osobowych, kontrole GIODO, bezpieczeństwo danych, rola administratora bezpieczeństwa informacji, egzekwowanie przepisów, pozwy grupowe czy przekazywanie danych osobowych poza Europejski Obszar Gospodarczy. Organizatorem Spotkania była Privacy Laws & Business.

**12. Spotkanie w Akademii Obrony Narodowej** (Warszawa, 13 kwietnia 2012 r.)

Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład dla studentów studiów doktorskich i kadry naukowo-dydaktycznej Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej.



Tematem wystąpienia był projekt zmian w prawie ochrony danych osobowych Unii Europejskiej przedstawiony przez Komisję Europejską w dniu 25 stycznia 2012 r., a także wyzwania stojące przed organem ds. ochrony danych osobowych wobec rozwoju nowych technologii. GODO omówił w szczególności zagadnienia przetwarzania danych osobowych w systemach monitoringu wizyjnego, przetwarzanie danych biometrycznych i profilowanie osób.

**13. VI Europejska Konferencja Dyrektorów Przedszkoli pt. „Kontrola przedszkola kreatywnego”** (Warszawa, 26 kwietnia 2012 r.)

Miesięcznik „Dyrektor Szkoły” oraz kwartalnik „Przed Szkołą. Poradnik dyrektora przedszkola”, kontynuując misję informowania o zmianach w prawie oraz prowadzenia dyskusji ze środowiskiem kadry kierowniczej przedszkoli, zorganizowało Konferencję poświęconą zagadnieniu kontroli. Przedstawiciel GODO przedstawił uczestnikom kwestie dotyczące kontroli Generalnego Inspektora Ochrony Danych Osobowych w placówkach oświatowych oraz odpowiedzialności dyrektorów, jako administratorów danych osobowych.

**14. Konferencja sekretarzy gmin, miast i powiatów województwa podkarpackiego** (Jasionka k/Rzeszowa, 7 maja 2012 r.)

Spotkanie z sekretarzami było okazją do wyjaśnienia wątpliwości związanych z właściwą interpretacją przepisów o ochronie danych osobowych, które powstają podczas realizacji wielu samorządowych zadań. Podczas tego wydarzenia przedstawiciele Generalnego Inspektora Ochrony Danych Osobowych przedstawili projekty nowych unijnych przepisów dotyczących ochrony danych osobowych oraz wymagania dotyczące bezpieczeństwa danych osobowych w systemach informatycznych. Organizatorem Konferencji był Małopolski Instytut Samorządu Terytorialnego i Administracji, czyli Krakowski oddział Fundacji Rozwoju Demokracji Lokalnej.

**15. 6. Międzynarodowa Konferencja Fundraisingu w Polsce** (Warszawa, 09-10 maja 2012 r.)

Polskie Stowarzyszenie Fundraisingu już po raz szósty zorganizowało Międzynarodową Konferencję Fundraisingu, której celem było podniesienie kwalifikacji związanych z umiejętnością efektywnego i etycznego pozyskiwania i wydatkowania funduszy przez organizacje pozarządowe. Generalny Inspektor Ochrony Danych Osobowych zasiadał w Komitecie Honorowym tego edukacyjnego wydarzenia, podczas którego - w jednej z sesji plenarnych – przedstawiciel GODO przedstawił referat pt. „Prawidłowe zarządzanie danymi osobowymi. Jak bezpiecznie posługiwać się bazami danych”.

**16. II Międzynarodowa Konferencja „Miasto monitorowane – personel, aspekty prawne i technika systemów CCTV”.** (Częstochowa, 17 maja 2012 r.)

Konferencja poruszała najważniejsze i najbardziej aktualne zagadnienia dotyczące miejskich systemów monitoringu wizyjnego, w szczególności zaś stanowisko samorządów wobec opracowanych przez GODO wymagań do projektu ustawy o monitoringu wizyjnym. Wstępne założenia do ogólnej regulacji w zakresie dotyczącym monitoringu zaprezentował przedstawiciel GODO. Organizatorem

tego wydarzenia była Częstochowska Straż Miejska, Akademia Monitoringu Wizyjnego oraz Krajowa Rada Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej z siedzibą w Częstochowie.

**17. VI Forum IAB Polska** (Warszawa, 23 maja 2012 r.)

„Marketing adaptacyjny, adoptujące się przedsiębiorstwa” - to hasło pod jakim odbywało się VI Forum IAB Polska, podczas którego Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Zróbmy w Polsce internetowy raj” poświęcony omówieniu możliwych zmian w prawie ochrony danych osobowych. Organizatorem tego corocznego wydarzenia był Związek Pracodawców Branży Internetowej IAB Polska.

**18. XII Forum ADO/ABI** (Warszawa, 23 maja 2012 r.)

XII Forum ADO/ABI poświęcone było kilku ważnym zagadnieniom. W pierwszej części spotkania omówione zostały najnowsze zmiany w europejskim prawie ochrony danych osobowych. W wykładzie wprowadzającym Generalny Inspektor Ochrony Danych Osobowych, przedstawił rezultaty pierwszego etapu prac nad nowymi ramami prawnymi ochrony danych osobowych w UE. Szczególne zainteresowanie wywołały tematy budzące kontrowersje w świetle orzecznictwa sądów administracyjnych oraz ostatnich zmian w ustawie o ochronie danych osobowych, a mianowicie przetwarzanie danych biometrycznych oraz przekazywanie danych do państw trzecich. Organizatorem Forum było Centrum Promocji Informatyki.

**19. VIII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych**  
(Zakopane, 23-25 maja 2012 r.)

Krajowe Stowarzyszenie Ochrony Informacji Niejawnych było organizatorem VIII Kongresu, który odbywał się pod patronatem honorowym GIODO. Wiodącym zagadnieniem tego wydarzenia była reforma ochrony prywatności i zasad przetwarzania danych stanowiących zasób informacyjny państwa. Uroczystego otwarcia Forum dokonał Zastępca Generalnego Inspektora Ochrony Danych Osobowych, który wygłosił wykład inauguracyjny dotyczący standardów stosowania w praktyce przepisów o ochronie danych osobowych i planowanych zmian w unijnym prawie.

**20. Seminarium „Skuteczne usługi w ubezpieczeniach społecznych”** (Warszawa, 24 maja 2012 r.)

Generalny Inspektor Ochrony Danych Osobowych wziął udział w seminarium zorganizowanym przez europejskie stowarzyszenie ISSA Polska, podczas którego w trakcie sesji poświęconej aspektom wiarygodności w e-usługach wygłosił wykład pt. „Bazy danych ubezpieczeń społecznych jako rejestry publiczne: Kwestie ochrony prywatności i poufności związane z interoperacyjną e-administracją”. GIODO uczestniczył również w dyskusji dotyczącej bezpieczeństwa, autoryzacji i podpisów elektronicznych oraz zyskiwania zaufania konsumenta.

**21. Spotkanie GIODO z przedstawicielami biznesu** (Warszawa, 25 maja 2012 r.)

Wskazaniu, jak w praktyce przedsiębiorcy powinni stosować zasady ochrony danych osobowych poświęcone było spotkanie GIODO z przedstawicielami biznesu, zorganizowane przez firmę Iron Mountain. Podczas spotkania omówione zostały różnorodne aspekty ochrony danych osobowych, które pojawiają się w codziennej działalności przedsiębiorców, m.in. przetwarzanie danych osobowych w grupie kapitałowej, przekazywanie danych do państw trzecich, zawieranie umów powierzenia przetwarzania danych osobowych czy możliwość korzystania z coraz powszechniejszego modelu biznesowego, jakim jest *cloud computing*. Uczestników spotkania ochrona danych osobowych interesowała też w kontekście kształtowania relacji z podwykonawcami, a także przetwarzanie danych osobowych na potrzeby rekrutacji, w tym pozyskiwanie referencji.

## **22. Seminarium „Zagrożenia i wyzwania w procesie przetwarzania danych osobowych w branży hotelarskiej” (Warszawa, 28 maja 2012 r.)**

Katedra Gospodarki Turystycznej, Hotelarstwa i Gastronomii Almamer – Szkoła Wyższa była organizatorem seminarium w ramach cyklu spotkań z serii „Nowe wyzwania edukacji turystycznej”. Podczas seminarium przedstawiciel GIODO wygłosił wykład „Zagrożenia i wyzwania w procesie przetwarzania danych osobowych w branży hotelarskiej”. W seminarium udział wzięli reprezentanci Izby Gospodarczej Hotelarstwa Polskiego, Warszawskiej Izby Turystyki, przedstawiciele hoteli oraz studenci.

## **23. Konferencja Naukowa „Cloud computing – przetwarzanie w chmurze” (Warszawa, 29 maja 2012 r.)**

Celem konferencji było kompleksowe omówienie kwestii przetwarzania danych przy zastosowaniu modelu biznesowego *cloud computingu*, perspektywy rozwoju tej technologii, możliwości jej wykorzystania przez przedsiębiorców i administrację publiczną, a także zagrożenia, jakie może stwarzać dla prywatności i ochrony danych osobowych. Zagadnienie *cloud computingu* analizowano biorąc pod uwagę aspekty prawne, socjologiczne, etyczne, ekonomiczne oraz technologiczne. Konferencja została zorganizowana przez Uniwersytet Kardynała Stefana Wyszyńskiego, Generalnego Inspektora Ochrony Danych Osobowych, Szefa Agencji Bezpieczeństwa Wewnętrznego oraz Naukowe Centrum Prawno – Informatyczne. Podczas tego wydarzenia odbyło się uroczyste wręczenie nagród studentom - laureatom konkursu na esej dotyczący ochrony danych osobowych kandydatów do pracy przetwarzanych w sieci informatycznej, którego organizatorem był GIODO przy wsparciu merytorycznym PricewaterhouseCoopers Legal Szurmińska-Jaworska sp.k.

## **24. Międzynarodowa Konferencja „Europejskie Forum Podpisu Elektronicznego” (Międzyzdroje, 4-6 czerwca 2012 r.)**

Generalny Inspektor Ochrony Danych Osobowych uczestniczył w międzynarodowej konferencji poświęconej zagadnieniom związanym z podpisem elektronicznym. W ramach bloku tematycznego poświęconego prawnym zagadnieniom standaryzacji, interoperacyjności i akredytacji, GIODO

wyłosił wykład pt. „Wpływ nowo promowanych zasad ochrony prywatności na działanie rynku cyfrowego w Europie. Szanse i zagrożenia płynące z 'privacy by design', przynależności danych, prawa do bycia zapomnianym i minimalizacji przetwarzania danych”. Organizatorem tego wydarzenia był Zachodniopomorski Uniwersytet Technologiczny w Szczecinie.

#### **25. Konferencja z cyklu „Siećpospolita” (Warszawa, 13 czerwca 2012 r.)**

Generalny Inspektor Ochrony Danych Osobowych, na zaproszenie Prezydenta Rzeczypospolitej Polskiej Pana Bronisława Komorowskiego, wziął udział w konferencji z cyklu „Siećpospolita”, w ramach Forum Debaty Publicznej pt. „Elektroniczne usługi administracji publicznej”. Spotkanie odbyło się w Pałacu Prezydenckim.

#### **26. III Międzynarodowa Konferencja Naukowa pt. „Współczesne bezpieczeństwo. Wymiar społeczny i jednostkowy” (Warszawa, 21 czerwca 2012 r.)**

Celem konferencji była prezentacja aktualnego stanu badań nad jednym z najistotniejszych wymiarów współczesnego bezpieczeństwa, jakim jest bezpieczeństwo społeczne oraz bezpieczeństwo jednostkowe – rozpatrywane w różnych płaszczyznach, kontekstach i perspektywach badawczych. Podczas konferencji Zastępca Generalnego Inspektora Ochrony Danych Osobowych wyłosił wykład pt. „Współczesne bezpieczeństwo – granice ochrony prywatności i prawa do ochrony danych osobowych”. Organizatorami tego wydarzenia byli: Instytut Nauk Społecznych Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Centralna Biblioteka Wojskowa oraz Siedleckie Towarzystwo Naukowe.

#### **27. VI Powszechny Zjazd Archiwistów Polskich (Wrocław, 5-7 września 2012 r.)**

Zagadnienia związane z ochroną informacji i danych osobowych w świetle rozwoju e-administracji w Polsce, zarządzaniem dokumentacją i koniecznością nadania archiwom postaci cyfrowej, były tematem dyskusji podczas tego wydarzenia. W ramach panelu „Ochrona informacji i danych osobowych” GIODO wyłosił wystąpienie pt. „Propozycje zmian w prawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych”. Organizatorami V Zjazdu byli: Stowarzyszenie Archiwistów Polskich i Naczelna Dyrekcja Archiwów Państwowych przy współpracy Politechniki Wrocławskiej.

#### **28. I Konferencja Zarządzania Ciągłością Działania „Zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów państwa w obliczu dzisiejszych zagrożeń” (Szczecino, 10-11 września 2012 r.)**

„Ocena skutków przedsięwzięcia dla ochrony prywatności (Privacy Impact Assessment) jako element systemu bezpieczeństwa ciągłości działania” to tytuł wystąpienia Generalnego Inspektora Ochrony Danych Osobowych podczas konferencji zorganizowanej przez Wyższą Szkołę Policji w Szczecinie oraz British Standard Institution Group. Jednym z celów tego wydarzenia było określenie płaszczyzny współpracy dla wszystkich poziomów administracji państwowej, służb mundurowych oraz

infrastruktury IT w zakresie wymiany, dostępności oraz poufności informacji, w związku z zapewnieniem bezpieczeństwa państwa i ciągłości funkcjonowania jego organów.

## **29. Konferencja „Inteligentne sieci – rynek, konsument i zasada zrównoważonego rozwoju”**

(Warszawa, 18 września 2012 r.)

Głównym celem konferencji było zaprezentowanie koncepcji budowy inteligentnych sieci energetycznych w Polsce. Ich rozwój i proces wdrażania jest pod szczególną obserwacją Generalnego Inspektora Ochrony Danych Osobowych, który aktywnie uczestniczy w pracach dotyczących stworzenia podstaw prawnych dla wprowadzenia całości rozwiązań *smart meteringu* w Polsce. Podczas konferencji przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych podkreślił, że skoro przy wdrażaniu technologii inteligentnego pomiaru oraz inteligentnych sieci wykorzystuje się najnowsze rozwiązania z zakresu informatyki i telekomunikacji, konieczne jest uwzględnianie mechanizmów i procedur służących ochronie danych osobowych już na etapie projektowania i tworzenia systemu. Wskazał ponadto na zagrożenia, jakie budowa inteligentnych sieci energetycznych może rodzić dla naszej prywatności i podkreślał potrzebę przeprowadzenia stosownej analizy w tym zakresie. Organizatorem tego wydarzenia był Urząd Regulacji Energetyki.

## **30. Konferencja „Nowoczesne technologie w procesie karnym i czynnościach wykrywczych a prawa i wolności obywatelskie”** (Warszawa, 20 września 2012 r.)

„Kwanty informacji o osobie. Prawne aspekty przetwarzania danych o osobach i ‘obiektach’ pochodzących z rozproszonych zbiorów” to tytuł wystąpienia GODO podczas konferencji zorganizowanej przez Sąd Najwyższy RP oraz Polską Platformę Bezpieczeństwa Wewnętrznego przy współpracy Helsińskiej Fundacji Praw Człowieka.

## **31. Konferencja Specjalistyczna pt. „Prawo, Licencje i Normy we współczesnej szkole”** (Warszawa, 24 września 2012 r.)

Podczas konferencji, GODO przedstawił prezentację nt. ochrony danych w oświacie, a także omówione zostały założenia i przebieg realizacji Programu edukacyjnego GODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”. Organizatorami konferencji byli Kuratorium Oświaty w Warszawie oraz Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

## **32. Kongres Contact Center** (Warszawa, 24-25 września 2012 r.)

Kongres poświęcony był praktycznym aspektom działalności firm telemarketingowych w kontekście budowy ich społecznego wizerunku. Podczas spotkania przedstawiciel GODO wygłosił referat „Zasady pozyskiwania i udostępniania danych osobowych w działalności telemarketingowej”, w którym przedstawił warunki legalnego pozyskiwania i wykorzystywania danych osobowych przez telemarketerów, podkreślając w szczególności konieczność spełnienia przez nich obowiązku informacyjnego wobec klientów Contact Center i realizację ich uprawnień kontrolnych, tj. prawa do

złożenia sprzeciwu wobec przetwarzania danych w celach marketingowych. Omówił także procedury bezpieczeństwa na etapie pozyskiwania, utrwalania, udostępniania i archiwizowania danych osobowych przetwarzanych w ramach Contact Center. Organizatorem Kongresu była Nowoczesna Firma S.A.

### **33. II Europejski Kongres Małych i Średnich Przedsiębiorstw** (Katowice, 26 września 2012 r.)

Celem Kongresu było zwiększenie świadomości i wiedzy przedsiębiorców w zakresie bezpieczeństwa informacji i ochrony danych osobowych. W sesji panelowej „Bezpieczeństwo informacji i ochrona danych osobowych w MŚP”, Zastępca Generalnego Inspektora Ochrony Danych Osobowych zapoznał uczestników z obowiązkami w zakresie ochrony danych osobowych, prowadzenia baz kontrahentów oraz z zagrożeniami w konkurencyjnej gospodarce rynkowej. Organizatorami Kongresu byli: Regionalna Izba Gospodarcza w Katowicach, Krajowa Izba Gospodarcza oraz Polska Agencja Rozwoju Przedsiębiorczości.

### **34. XVIII Forum Teleinformatyki „Polska w cyfrowej chmurze”** (Warszawa - Miedzeszyn, 27 września 2012 r.)

Przetwarzaniu danych osobowych w chmurze poświęcone było XVIII Forum Teleinformatyki, podczas którego GODO wygłosił referat „Budowa kompetencji cyfrowych w administracji publicznej”. Forum Teleinformatyki to najważniejsze spotkanie przedstawicieli administracji publicznej oraz środowiska naukowego i biznesowego zajmującego się prawnymi, ekonomicznymi i technicznymi aspektami informatyzacji administracji publicznej oraz telekomunikacji w sektorze publicznym. Jego 18. edycja objęta była patronatem Generalnego Inspektora Ochrony Danych Osobowych. Po raz czwarty do programu Forum włączona została sesja Forum Młodych Mistrzów, której celem jest popularyzacja w środowisku młodych naukowców ekonomicznych i prawnych zagadnień teleinformatyki w administracji publicznej. Udział w niej umożliwia studentom i młodym naukowcom zaprezentowanie efektów swych badań naukowych i działań praktycznych szerokiemu gronu specjalistów informatyków i menadżerów sektora publicznego.

### **35. Konferencja Edu Trendy 2012** (Warszawa, 28 września 2012 r.)

Problematyce zgodnego z prawem przetwarzania danych osobowych przez placówki oświatowe, w szczególności przepisom nowej ustawy o Systemie Informacji Oświatowej oraz procedurom stosowanym w tym zakresie przez przedszkola, poświęcona był konferencja Edu Trendy 2012. Przedstawiciele GODO omówili obowiązki i uprawnienia przedszkoli jako administratorów danych, w świetle kontroli przepisów o ochronie danych osobowych, a także zaprezentowane zostały założenia ogólnopolskiego Programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”. Organizatorami konferencji byli: Wolters Kluwer Polska, RedNet Media, Dyrektor Szkoły – Miesięcznik Kierowniczej Kadry Oświatowej oraz Przed Szkołą – Poradnik Dyrektora Przedszkola.

**36. Konferencja „EUROPOL – zwalczanie poważnej i zorganizowanej przestępczości w Europie.**

**Ochrona informacji i danych osobowych”** (Koszalin, 29-30 września 2012 r.)

Głównym celem konferencji było przedstawienie praktycznych możliwości współpracy różnych służb ochrony porządku prawnego z Europol oraz wymiana dotychczasowych doświadczeń w tym zakresie, w szczególności w kontekście zapewnienia właściwej ochrony informacji przed nieuprawnionym dostępem. „Ochrona danych osobowych w międzynarodowej wymianie informacji organów ścigania” to tytuł wystąpienia przedstawiciela Generalnego Inspektora Ochrony Danych Osobowych. Organizatorem konferencji było Biuro Międzynarodowej Współpracy Policji KGP we współpracy z Komendą Główną Straży Granicznej.

**37. Konferencja „Twoje dane – twoja sprawa. Prawo do prywatności i ochrony danych osobowych we współczesnej szkole”** (Warszawa, 8 października 2012 r.)

Konferencja zainaugurowała III edycję Ogólnopolskiego Programu Edukacyjnego GIODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”, objętego patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka. W programie konferencji poruszane były zagadnienia związane z ochroną danych osobowych w szkole, rolą dyrektora szkoły, a także prezentowano przykłady dobrych praktyk w podejmowaniu inicjatyw edukacyjnych przez jednostki administracji publicznej, samorządu terytorialnego czy organizacji pozarządowych. Podczas konferencji odbyły się warsztaty programowe połączone z przeprowadzeniem lekcji pokazowej. „Ochrona danych osobowych w szkole” to tytuł wykładu Generalnego Inspektora Ochrony Danych Osobowych, organizatora tego wydarzenia.

**38. Seminarium „Kto na nas patrzy? Obywatel pod obserwacją kamer”** (Warszawa, 11 października 2012 r.)

Seminarium poświęcone było zagadnieniom związanym ze stosowaniem systemów monitoringu i zagrożeniom, jakie one stwarzają dla prywatności osób fizycznych. Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład pt. „Kiedy struś włoży głowę w piasek, czyli co widać gdy patrzymy w oko kamery wideomonitoringu”, w którym wskazywał na pilną potrzebę uregulowania monitoringu w odrębnym akcie prawnym, innym niż ustawa o ochronie danych osobowych. Dzięki temu możliwe byłoby m.in. zagwarantowanie odpowiedniego standardu ochrony informacji pozyskiwanych z wykorzystaniem monitoringu. Organizatorami seminarium byli Rzecznik Praw Obywatelskich, GIODO i Fundacja Panoptykon.

**39. Konferencja „Cloud computing – biznes w chmurze”** (Warszawa, 16 października 2012)

Bezpieczeństwo danych w chmurze oraz regulacje gwarantujące ich bezpieczeństwo z punktu widzenia biznesu, to tematy poruszone w wystąpieniu GIODO podczas konferencji poświęconej modelowi przechowywania danych w chmurze. Organizatorem tego wydarzenia, któremu patronował Generalny Inspektor Ochrony Danych Osobowych, był Dziennik Gazeta Prawna.

#### **40. Spotkanie GIODO z przedsiębiorcami** (Warszawa, 16 października 2012 r.)

Rozwiązaniu problemów z praktycznym stosowaniem zasad ochrony danych osobowych w sektorze biznesu poświęcone było Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z przedsiębiorcami, podczas którego dr Wojciech R. Wiewiórowski, GIODO, przedstawił podstawy planowanej reformy unijnych przepisów w zakresie ochrony danych osobowych oraz omówił zmiany, jakie w związku z tzw. ustawą deregulacyjną już wkrótce mogą nastąpić w polskich przepisach. Część spotkania poświęcono wyjaśnieniu problemów związanych ze stosowaniem zasad ochrony danych osobowych w praktyce, jak kwestie udostępniania przez podmioty prywatne danych osobowych organom publicznym, przekazywania danych do państw spoza Europejskiego Obszaru Gospodarczego, czy nadawania upoważnień do przetwarzania danych osobowych. Organizatorem Spotkania była Firma Iron Mountain.

#### **41. Seminarium w ramach projektu „Obywatele i wybory”** (Warszawa, 17 października 2012 r.)

Fundacja im. Stefana Batorego była organizatorem cyklu eksperckich seminariów „Obywatele i wybory”, których celem było przedyskutowanie problemów związanych z udziałem obywateli w wyborach i wypracowanie rekomendacji. Staną się one potem podstawą działań rzeczniczych organizacji skupionych w koalicji „Masz Głos, Masz Wybór”. Seminarium zorganizowane 17 października 2012 r. poświęcone było zagadnieniom wykorzystania nowoczesnych technologii w wyborach (e-głosowanie, elektroniczny rejestr wyborców) oraz kwestii przejrzystości wyborów (finansowanie kampanii, obserwacje wyborów, itp.). Generalny Inspektor Ochrony Danych Osobowych oraz jego przedstawiciele uczestniczyli w roboczej dyskusji ekspertów na tematy poruszane podczas tego spotkania.

#### **42. XII edycja seminarium „Jakość danych w systemach ubezpieczeń społecznych”** (Warszawa, 18 października 2012 r.)

Tematem przewodnim tego wydarzenia było skuteczne i bezpieczne zarządzanie procesami gromadzenia i wymiany informacji, w powiązaniu z procesami biznesowymi, jak likwidacja szkód oraz związane z nią przeciwdziałanie przestępczości ubezpieczeniowej. Wiele uwagi poświęcono kwestiom zapewnienia należytej i zgodnej z prawem ochrony danych osobowych, która jest integralnym składnikiem zapewnienia wymaganej jakości danych w systemach informacyjnych zakładów ubezpieczeń. Podczas seminarium referat pt. „Ocena skutków przedsięwzięcia dla ochrony prywatności (Privacy Impact Assessment) wygłosił Generalny Inspektor Ochrony Danych Osobowych.

#### **43. Debata „Od Administratora do Inspektora”** (Warszawa, 19 października 2012 r.)

Debata na temat przyszłości funkcji Administratora Bezpieczeństwa Informacji (ABI) „Od Administratora do Inspektora“ dotyczyła zagadnień związanych z zapewnieniem niezależności stanowiska ABI, zakresem jego nowych obowiązków i odpowiedzialności, wymaganych kwalifikacji oraz rejestracji przez GIODO. W trakcie dyskusji Generalny Inspektor Ochrony Danych Osobowych



zwrócił uwagę na ewolucję statusu i funkcji ABI związanych z zaproponowanym w styczniu 2012 r. przez Komisję Europejską projekcie ogólnego rozporządzenia o ochronie danych oraz projekcie ustawy deregulacyjnej. Organizatorem debaty było Stowarzyszenie Administratorów Bezpieczeństwa Informacji oraz Generalny Inspektor Ochrony Danych Osobowych.

**44. Konferencja „Internetowa Publikacja Orzeczeń Sądowych – prawo do sądu i informacji publicznej”** (Warszawa, 24 października 2012 r.)

Głównym tematem konferencji była kwestia funkcjonalności uruchomionego z dniem 1 sierpnia 2012 r. Portalu Orzeczeń Sądów Powszechnych oraz zagadnienia związane z bezpieczeństwem teleinformatycznym, ochroną danych osobowych i ujednoliceniem linii orzeczniczej w ramach publikacji orzeczeń. Przedstawiciel GODO wygłosił referat poświęcony ochronie danych osobowych w obszarze działań związanych z publikacją orzeczeń sądowych. Organizatorem konferencji było Ministerstwo Sprawiedliwości.

**45. VI Forum Komunikacji Publicznej** (Łódź, 24 października 2012 r.)

Celem Forum było przekazanie informacji o trendach i zmianach na rynku komunikacji miejskiej ze szczególnym uwzględnieniem systemów dystrybucji biletów i elektronicznych usług miejskich. Podczas Forum przedstawiciel GODO wygłosił referat pt. „Zasady niezbędności danych osobowych dla potrzeb realizacji określonych celów oraz bezpieczeństwo i przetwarzanie danych osobowych w kontekście usług świadczonych w transporcie publicznym”. Organizatorem tego spotkania była Mennica Polska S.A.

**46. Konferencja „Operator Informacji Pomiarowych – nowe narzędzie na rynku energii”** (Warszawa, 25 października 2012 r.)

Konferencja miała na celu zaprezentowanie przedsiębiorstwom energetycznym oraz podmiotom odpowiedzialnym za organizację tego rynku, nowych uregulowań prawnych i rozwiązań w zakresie informacji pomiarowych i Operatora Informacji Pomiarowych. Podczas tego spotkania przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych wygłosił wykład „Regulacje prawne w ustawodawstwie krajowym dotyczące ochrony prywatności – w rozumieniu ustawy o ochronie danych osobowych”. Organizatorem tego wydarzenia była Spółka Energy Management and Conservation Agency.

**47. II Konferencja i Narodowy Test Interoperacyjności Podpisu Elektronicznego „CommonSign Warsaw 2012”** (Warszawa, 25-26 października 2012 r.)

Konferencja, która składa się z części testowej i teoretycznej, adresowana jest głównie do podmiotów zajmujących się dostawą aplikacji i usług z zakresu podpisu elektronicznego. Celem tej imprezy była weryfikacja i sprawdzanie interoperacyjności produktów służących upowszechnianiu podpisu elektronicznego w obszarze administracji i biznesu. Referat pt. „Wielość standardów podpisu

elektronicznego w praktyce – zaletą czy przeszkodą w implementacji” wygłosił przedstawiciel GODO. Organizatorem konferencji był Instytut Maszyn Matematycznych i Medien Service.

**48. Konferencja „Rozwój elektronicznej administracji w samorządach województwa mazowieckiego wspomagającej niwelowanie dwudzielności potencjału województwa”**  
(Warszawa, 5 listopada 2012 r.)

Generalny Inspektor Ochrony Danych Osobowych uczestniczył w konferencji na zaproszenie Marszałka Województwa Mazowieckiego - Pana Adama Struzika. W wystąpieniu dla uczestników reprezentujących urzędy powiatowe i gminne z województwa mazowieckiego, GODO wskazał, jak wiele zagrożeń dla danych osobowych niesie za sobą e-government.

**49. 4. Konferencja „Cloud 2012: Mobilność, wirtualizacja, cloud”** (Warszawa, 8 listopada 2012 r.)

Organizatorem czwartej edycji konferencji poświęconej zagadnieniu chmury obliczeniowej było czasopismo Computerworld. Generalny Inspektor Ochrony Danych Osobowych zainaugurował spotkanie wystąpieniem omawiającym zmiany prawne dotyczące przetwarzania w chmurze, jakie były w tym czasie przedmiotem prac organów administracji krajowej i UE. Odpowiadał także na pytania uczestników konferencji dotyczące m.in. bezpieczeństwa danych w chmurze oraz wytycznych GODO w zakresie stosowania rozwiązań chmurowych.

**50. XVI Międzynarodowa Konferencja Energetyczna EUROPOWER** (Warszawa, 7-8 listopada 2012 r.)

Kluczowe zmiany otoczenia prawnego w sektorze energetycznym z perspektywy administracji rządowej, regulatora i firm energetycznych, a także wyzwania inteligentnego rynku, były tematem wiodącym XVI Międzynarodowej Konferencji Energetycznej EUROPOWER, podczas której Generalny Inspektor Ochrony Danych Osobowych wygłosił prezentację pod tytułem „Czy zagrożenie cyberataku na sieci energetyczne w Polsce jest realne?”.

**51. IX Doroczna Konferencja PPBW „Nowe kierunki badań nad bezpieczeństwem wewnętrznym oraz ich praktyczne wykorzystanie ”** (Będlewo k/Poznań, 4-7 grudnia 2012 r.)

Celem IX Konferencji zorganizowanej przez Polską Platformę Bezpieczeństwa Wewnętrznego (PPBW) były kwestie związane z wykorzystywaniem nowoczesnych technologii przez służby odpowiedzialne za bezpieczeństwo państwa i jego obywateli. Przedstawione zostały zarówno projekty rozwojowe realizowane w ramach PPBW, jak i przewidywane kierunki dalszych prac badawczych prowadzonych przez polskie uczelnie wyższe w obszarze bezpieczeństwa wewnętrznego. Istotnym zagadnieniem poruszonym podczas konferencji była kwestia związana z wdrożeniem systemu Automatycznego Rozpoznawania Mowy (ARM) do pracy służb mundurowych, w szczególności policji, która przewiduje m. in. zintegrowanie systemu ARM z aplikacją e-posterunek, a także w innych instytucjach, np. w wymiarze sprawiedliwości. Generalny Inspektor Ochrony Danych Osobowych był uczestnikiem między innymi dyskusji na temat koncepcji budowy zaawansowanej architektury

Zintegrowanej Platformy Teleinformatycznej, opartej na modelu obliczeniowym *cloud computing*, przy zastosowaniu tzw. chmury prywatnej.

**52. Konferencja naukowa „Dokumentacja elektroniczna w podmiotach publicznych** (Warszawa, 6 grudnia 2012 r.)

Elektroniczne zarządzanie dokumentacją w administracji publicznej i jej długotrwałe przechowywanie, możliwość korzystania przez urzędy z *cloud computingu* oraz stosowanie rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, były przedmiotem debaty podczas konferencji zorganizowanej przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Generalnego Inspektora Ochrony Danych Osobowych, Naczelną Dyрекcję Archiwów Państwowych oraz Naukowe Centrum Prawno-Informatyczne. Wykład Generalnego Inspektora Ochrony Danych Osobowych pt. „Wielki Brat i jego urzędowe Małe Siostry. Urząd, *jego* dane, informacje, dokumenty i rejestry publiczne” rozpoczął obrady konferencji. W czasie jej trwania został również rozstrzygnięty konkurs z cyklu Forum Młodych Mistrzów, skierowany dla młodych naukowców oraz studentów. Nagrodą dodatkową w tym Konkursie przyznaną przez Generalnego Inspektora Ochrony Danych Osobowych była nagroda indywidualna dla najlepszego mówcy za sposób prezentowania swojej pracy naukowej.

**53. Kongres Akademickich Biur Karier** (Warszawa, 6 grudnia 2012 r.)

Kongres Akademickich Biur Karier i jednostek uczelnianych odpowiedzialnych za monitoring zawodowych losów absolwenta, odbywał się pod hasłem „Monitorowanie karier zawodowych absolwentów – dobre praktyki”. Przedstawiciel GODO wystąpił w roli prelegenta z prezentacją poświęconą przestrzeganiu zasad ochrony danych osobowych w procesie monitorowania losów zawodowych absolwentów. Organizatorem tego wydarzenia byli: Uniwersytet Warszawski, Rzecznik Praw Absolwenta oraz Ministerstwo Nauki i Szkolnictwa Wyższego.

**54. Spotkanie z Panem Giovannim Buttarellim, Zastępcą Europejskiego Rzecznika Ochrony Danych Osobowych** (Warszawa, 12 grudnia 2012 r.)

Spotkanie z Panem Giovannim Buttarellim, Zastępcą Europejskiego Rzecznika Ochrony Danych Osobowych, poświęcone było zagadnieniom praktycznego wpływu ogólnego rozporządzenia o ochronie danych na prawodawstwo krajów członkowskich UE i prowadzone było w formule sesji eksperckiej z udziałem przedstawicieli Europejskiego Rzecznika Ochrony Danych Osobowych, Generalnego Inspektora Ochrony Danych Osobowych, zainteresowanych ministerstw oraz przedstawicieli Sejmu i Senatu. Podczas spotkania dyskutowane były następujące zagadnienia: rola ogólnego rozporządzenia o ochronie danych osobowych, jako aktu prawa europejskiego bezpośrednio obowiązującego, bezpośrednio stosowanego i bezpośrednio skutecznego w państwach członkowskich UE; kształt przyszłej regulacji krajowej dotyczącej organu ochrony danych osobowych oraz kontroli

sądowej ochrony danych osobowych; sytuacja, w której obecnie obowiązujące prawo krajowe przewiduje wyższe standardy ochrony danych osobowych niż projekt nowego rozporządzenia (np. przepisy szczególne Kodeksu pracy); przypadki przenikania się ochrony danych osobowych z ochroną tajemnic prawnie chronionych, np. tajemnicą bankową, telekomunikacyjną); zasady notyfikowania odrębności prawnych istniejących w krajach członkowskich UE; skuteczności systemu sankcji administracyjnych proponowanych w projekcie ogólnego rozporządzenia o ochronie danych osobowych. Organizatorem tego wydarzenia był Generalny Inspektor Ochrony Danych Osobowych.

### **7.2.8. Porozumienia o współpracy**

#### **a) Porozumienie o współpracy GIODO z Wyższą Szkołą Informatyki i Zarządzania z siedzibą w Rzeszowie, 08.05.2012 r.**

W siedzibie Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie zawarte zostało porozumienie o współpracy między uczelnią a GIODO, podpisane przez prof. dr hab. Jerzego Chłopeckiego, prorektora ds. nauki WSiIZ i Pana Andrzeja Lewińskiego, zastępcę Generalnego Inspektora Ochrony Danych Osobowych. Podczas uroczystości obecni byli także dr inż. Andrzej Mantaj, dyrektor Centrum Studiów Podyplomowych WSiIZ oraz Pan Andrzej Kaczmarek, dyrektor Departamentu Informatyki Biura GIODO. Porozumienie dotyczy współpracy w zakresie ochrony prywatności i danych osobowych. Przewiduje m.in. wspólną organizację seminariów, konferencji, szkoleń i praktyk zawodowych oraz realizację prac naukowych i badawczych z zakresu ochrony danych osobowych.

#### **b) Porozumienie o współpracy GIODO z Polskim Związkiem Przemysłu Motoryzacyjnego, 16.XI.2012 r.**

Porozumienie o współpracy GIODO z Polskim Związkiem Przemysłu Motoryzacyjnego (PZPM) na rzecz podwyższania poziomu wiedzy zawodowej i profesjonalnych umiejętności praktycznych w zakresie ochrony danych osobowych i prawa do prywatności, podpisali dr Wojciech Rafał Wiewiórowski, GIODO i Pan Jakub Faryś, Prezes Polskiego Związku Przemysłu Motoryzacyjnego (PZPM). Integralną częścią podpisanego porozumienia obu instytucji był dokument „Kodeks dobrych praktyk w zakresie ochrony danych osobowych klientów i potencjalnych klientów” opracowany przez PZPM we współpracy z GIODO w formie praktycznego przewodnika.

#### **c) Porozumienie o współpracy GIODO z Wyższą Szkołą Zarządzania i Bankowości w Krakowie, 24.11.2012 r.**

W siedzibie Wyższej Szkoły Zarządzania i Bankowości w Krakowie w dniu 24 listopada 2012 r. zawarte zostało porozumienie o współpracy edukacyjnej i szkoleniowej między uczelnią

a Generalnym Inspektorem Ochrony Danych Osobowych. W imieniu szkoły podpisał je prof. dr hab. inż. Włodzimierz Roszczyniański – Rektor uczelni, a ze strony GIODO – dr Wojciech Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, który wygłosił wykład inauguracyjny I edycji studiów podyplomowych „Ochrona danych osobowych i informacji prawnie chronionych w administracji i biznesie”. To już kolejne porozumienie, jakie zawiera GIODO ze szkołą wyższą w celu uruchomienia studiów podyplomowych. W programie studiów organizowanych przez WSZiB w Krakowie znajdują się m.in. następujące zagadnienia: ochrona danych osobowych, cyberterroryzm i zagrożenia bezpieczeństwa informacji w cyberprzestrzeni, bezpieczeństwo systemów i sieci teleinformatycznych, zasady ochrony informacji niejawnych w Polsce.

**d) Porozumienie w sprawie zasad współdziałania GIODO z Państwową Inspekcją Pracy, 14.12.2012 r.**

W dniu 14 grudnia 2012 r. w Warszawie, dr Wojciech R. Wiewiórowski, GIODO i Pani Iwona Hickiewicz, Główny Inspektor Pracy, podpisali porozumienie w sprawie zasad współdziałania obu instytucji w realizacji ustawowych zadań dla podniesienia skuteczności działań na rzecz przestrzegania przepisów o ochronie danych osobowych w stosunkach pracy. Porozumienie to ma w dużej mierze charakter edukacyjny, gdyż przewiduje m.in. wzajemną wymianę doświadczeń wynikających z kontroli realizowanych przez każdą ze stron porozumienia zgodnie z przyznanymi jej kompetencjami, współpracę przy podejmowaniu działań na rzecz podnoszenia kwalifikacji pracowników obu instytucji poprzez np. wspólne opracowywanie programów szkoleń czy wymianę wykładowców, a także konsultacje w zakresie doskonalenia metodyki prowadzenia kontroli.

## **7.2.9. Inne informacje**

**a) Przedstawiciel GIODO w Radzie Programowej Podyplomowego Studium Ochrony Danych Osobowych Uniwersytetu Łódzkiego**

Pan Andrzej Lewiński, Zastępca Generalnego Inspektora Ochrony Danych Osobowych, wszedł w skład Rady Programowej Podyplomowego Studium Ochrony Danych Osobowych. Utworzenie na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego dwusemestralnego Podyplomowego Studium Ochrony Danych Osobowych to efekt porozumienia o współpracy zawartego między tą uczelnią a GIODO 8 grudnia 2011 r. Przewidywało ono m.in. wspólną realizację przedsięwzięć na rzecz podnoszenia wiedzy w zakresie ochrony danych osobowych. W 2012 roku plany weszły w fazę realizacji - uczelnia opracowała ramowy program studium i powołała jego radę programową. W jej skład, oprócz ministra Andrzeja Lewińskiego, weszli przedstawiciele Wydziału Prawa i Administracji UŁ: prof. nadzw. dr

hab. Zofia Duniewska, prof. nadzw. dr hab. Zbigniew Góral, prof. nadzw. dr hab. Teresa Wyka oraz dr Ewa Kulesza (pierwszy Generalny Inspektor Ochrony Danych Osobowych).

**b) Trwają prace nad Kodeksem dobrych praktyk dla organizacji pozarządowych**

Organizacje pozarządowe prowadzą z przedstawicielami Generalnego Inspektora Ochrony Danych Osobowych konsultacje, które mają na celu wypracowanie Kodeksu dobrych praktyk z zakresu ochrony danych osobowych. Z uwagi na obowiązujące przepisy prawa krajowego i europejskiego oraz przyjęte standardy pracy z klientem, podmioty te uznają konieczność zapewnienia ochrony danych osobowych i prywatności osób korzystających z nieodpłatnej pomocy psychologicznej, prawnej, rzeczowej i innej świadczonej przez różne organizacje pozarządowe. Pierwsze spotkanie robocze dotyczące tego kodeksu zorganizowane zostało 11 kwietnia 2012 r. w siedzibie GIODO. Wstępną wersję projektu tego poradnika przygotowała Fundacja Dzieci Niczyje. W grupie roboczej konsultującej zakres uregulowania oraz kształtu projektu kodeksu, znaleźli się przedstawiciele następujących organizacji pozarządowych: Stowarzyszenie Interwencji Prawnej, Fundacja Academia Iuris, Stowarzyszenie Karan, Komitet Ochrony Praw Dziecka, Stowarzyszenie SOS dla Rodziny, Centrum Praw Kobiet, Ogólnopolskie Pogotowie dla Ofiar Przemocy w Rodzinie "Niebieska Linia" oraz Fundacja Dzieci Niczyje.

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

Podobnie, jak w latach poprzednich, również w 2012 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 GIODO była zwrócona szczególnie na prace podejmowane przez Komitet JTC/SC27 w ramach grupy roboczej WG 5 - Identity Management and Privacy Technologies. W roku 2012 w ramach ww. Komitetu Technologicznego Nr 182 przygotowanych zostało 60 projektów norm.

**8. 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 i spotkaniach 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 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). W latach 2011-2012 prace Komitetu T-PD koncentrowały się w szczególności 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.

Rezultatem społecznych konsultacji przeprowadzonych w ostatnich latach przez Radę Europy, a także prac prowadzonych przez Biuro Komitetu T-PD, był dokument pt. „Modernisation of Convention 108: proposals”. Podczas 28. plenarnego posiedzenia Komitetu T-PD w dniach 19-20 czerwca 2012 r. odbyło się drugie czytanie propozycji zmian do Konwencji nr 108. Ostatecznie dokument ten został zatwierdzony na 29. plenarnym zebraniu Komitetu T-PD, który odbył się w dniach 29-30 listopada 2012 r. w Strasburgu i przekazany do Komitetu Ministrów Rady Europy. Dokument przewiduje zmiany dążące w kierunku:

- zachowania istniejących przepisów Konwencji, jak również dodaje bardziej szczegółowe zapisy, w tym aktualizację terminologii oraz wprowadzenie pewnych nowych zasad, jak np. zasady rozliczalności;
- zachowania spójności i zgodności przepisów z ustawodawstwem Unii Europejskiej;
- zapewnienia, aby Konwencja była nadal neutralna pod względem technologicznym;
- potwierdzenia potencjału Konwencji, jako uniwersalnego standardu o otwartym charakterze;
- zapewnienia Konwencji efektywności środków oraz prostoty sformułowania zasad;
- zachowania zasady, zgodnie z którą przepisami Konwencji objęte są podmioty zarówno sektora publicznego, jak i prywatnego.

Polski organ ds. ochrony danych uczestniczy w pracach Wspólnego Organu Nadzorczego zajmującego się zagadnieniami ochrony danych osobowych w Systemie Informacyjnym Schengen

(WON Schengen)<sup>237</sup>, Wspólnego Organu Nadzorczego nad Europolem (WON Europolu)<sup>238</sup>, a także Wspólnego Organu Nadzorczego właściwego w sprawach ochrony danych osobowych w Systemie Informacji Celnej (WON ds. Celnych)<sup>239</sup>, którego wiceprzewodniczącym w dniu 4 października 2012 r. został wybrany Piotr Drobek, Zastępca Dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej Biura GODO. Ponadto, GODO bierze aktywny udział w pracach grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac, Systemem Informacji Celnej oraz nowopowołanej grupy koordynacyjnej do spraw nadzoru nad systemem VIS. W trakcie Wiosennej Konferencji Europejskich Rzeczników Ochrony Danych w dniach 3 - 4 maja 2012 r. w Luksemburgu zdecydowano o zaprzestaniu działalności przez Grupę roboczą ds. policji i wymiaru sprawiedliwości, w której pracach w poprzednich latach również uczestniczył polski organ ochrony danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych uczestniczy także w odbywających się cyklicznie dwa razy do roku spotkaniach Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji (tzw. Grupy Berlińskiej)<sup>240</sup>, a w dniach 23-24 kwietnia 2012 r. w Sopocie był gospodarzem 51. Spotkania Grupy Berlińskiej. Problematyka sopockich obrad koncentrowała się wokół przetwarzania danych przy zastosowaniu rozwiązań typu *cloud computing*, realizacji prawa do bycia zapomnianym oraz profilowania użytkowników Internetu przez firmy marketingowe poprzez stosowanie specjalnych narzędzi analitycznych. Za duże osiągnięcie tego Spotkania uznać należy przyjęcie dokumentu roboczego będącym wspólnym stanowiskiem Grupy na temat zasad ochrony prywatności w przypadku przetwarzania danych przy użyciu chmury obliczeniowej, nazwanego **Memorandum Sopockim**.

W omawianym roku sprawozdawczym 2012, podobnie jak w latach poprzednich, na szczególne podkreślenie zasługuje współpraca Generalnego Inspektora z innymi organami ochrony danych osobowych w ramach **Grupy Roboczej Art. 29 ds. ochrony danych osobowych**<sup>241</sup> (GR Art. 29), powołanej na mocy art. 29 ww. dyrektywy 95/46/WE. W skład tego organu wchodzi przedstawiciele krajowych organów ochrony danych z państw członkowskich UE, przedstawiciel Komisji Europejskiej

---

<sup>237</sup> Więcej informacji jest dostępnych na stronie internetowej: <http://schengen.consilium.europa.eu/about/tasks-of-the-jsa-schengen.aspx?lang=pl>

<sup>238</sup> Więcej informacji jest dostępnych na stronie internetowej: <http://europoljsb.consilium.europa.eu/about.aspx?lang=pl>

<sup>239</sup> Wspólny Organ Nadzorczy ds. Celnych to organ nadzoru ustanowiony na podstawie art. 25 decyzji Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych. WON ds. Celnych prowadzi nadzór i zapewnia, by podczas przetwarzania danych osobowych za pomocą systemu informacji celnej stosowane były przepisy ww. decyzji oraz decyzji ramowej 2008/977/WSiSW pod względem ochrony osób fizycznych. W skład Wspólnego Organu Nadzorczego ds. Celnych wchodzi po dwóch przedstawicieli organu bądź organów ochrony danych każdego z Państw Członkowskich będących stronami Konwencji o zastosowaniu technologii informatycznych dla celów celnych.

<sup>240</sup> Grupa Berlińska, której nazwa związana jest z tym, że jej pracom - od chwili utworzenia 1983 r. - przewodniczy Berliński Rzecznik Ochrony Danych Osobowych i Dostępu do Informacji, skupia ekspertów z zakresu technologii komunikacyjnych, informatyki i ochrony danych osobowych. Wynikami jej pracy są tzw. wspólne stanowiska w zakresie wymagań i warunków, jakie powinny być spełniane zarówno przez produkty wytwarzane przez dostawców technologii, jak i podmioty, które używają tych produktów, np. operatorów telekomunikacyjnych, administratorów portali informacyjnych, stron internetowych czy też podmiotów, którzy z produktów tych korzystają jako użytkownicy końcowi.

<sup>241</sup> [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm)



oraz Europejski Inspektor Ochrony Danych Osobowych. Do zadań Grupy należy badanie wszelkich kwestii dotyczących stosowania krajowych środków przyjętych na mocy dyrektywy 95/46/WE, tak by przyczyniały się do jednolitego stosowania tych środków, przekazywanie Komisji Europejskiej opinii na temat stopnia ochrony danych osobowych we Wspólnocie i w państwach trzecich, doradzanie w sprawie wszelkich proponowanych zmian tejże dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i swobód osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych środków wspólnotowych dotyczących tych praw i wolności, a także wydawanie opinii na temat kodeksów postępowania opracowywanych na poziomie wspólnotowym. Zadania te mają zastosowanie także w odniesieniu do sektora łączności elektronicznej, w oparciu o przepis art. 15 ust. 3 dyrektywy 2002/58/WE. Grupa Robocza realizuje te zadania wydając rekomendacje, opinie i dokumenty robocze.

W roku sprawozdawczym 2012 Generalny Inspektor Ochrony Danych Osobowych uczestniczył we wszystkich posiedzeniach wspomnianej Grupy.

Podczas 84 posiedzenia GR Art. 29, które odbyło się w dniach 1 – 2 lutego 2012 r. odbyły się wybory na jej Przewodniczącego. Ponownie został nim Pan Jacob Kohnstamm, z holenderskiego organu ochrony danych. Natomiast Pan Igor Nemec, Przewodniczący Urzędu Ochrony Danych Osobowych Republiki Czeskiej oraz Christopher Graham, Rzecznik Informacji Zjednoczonego Królestwa, zostali powołani do pełnienia funkcji Wiceprzewodniczących. Zarówno kadencja Przewodniczącego, jak i Wiceprzewodniczących, trwa dwa lata.

GR Art. 29 przyjęła również Program prac na lata 2012-2013 (WP 190)<sup>242</sup>. Podkreślono w nim, że celem GR Art. 29 będzie nie tylko zapewnienie spójnego i prawidłowego stosowania istniejących ram prawnych w zakresie ochrony danych osobowych, ale także przygotowania do przyjęcia przyszłych ram prawnych zaproponowanych przez Komisję Europejską w dniu 25 stycznia 2012 r. Wśród nich znalazła się wykładnia kluczowych przepisów, jak zasada celowości (zmiana z „określenia celu” na „wykorzystanie zgodnie z celem” i wskazanie ewentualnych wyjątków), uwzględnienie innych podstaw przetwarzania skoncentrowanych na „uzasadnionym interesie”, monitorowanie wdrożenia dyrektywy o prywatności i łączności elektronicznej, a także zapewnienie spójności z innymi ramami ochrony danych (OECD, Rada Europy). W Programie zwrócono także uwagę, że innowacje i rozwój technologiczny, zwłaszcza w środowisku internetowym, wciąż stanowią wyzwanie dla ochrony danych osobowych (wykorzystanie chmur obliczeniowych, techniki rozpoznawania twarzy, śledzenie za pomocą identyfikacji urządzeń czy wytyczne dotyczące aplikacji do smartfonów), i że należy doprecyzować i wzmocnić rolę wszystkich zainteresowanych podmiotów w obszarze ochrony danych – tj. osób, których dane dotyczą, administratorów danych i organów ochrony danych.

---

<sup>242</sup> Dokumenty przyjęte przez Grupę Roboczą Art. 29 w wersji elektronicznej dostępne są na stronie internetowej: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm)

Przyjęty dokument obliguje GR Art. 29 do zapewnienia spójności i skuteczności w podejściu do ochrony danych osobowych w obszarze wolności, bezpieczeństwa i sprawiedliwości (unijny system śledzenia przepływu środków finansowych służących do finansowania terroryzmu, ocena wdrożenia decyzji ramowej 2008/977/WSiSW, przyszły nadzór w ramach dawnego trzeciego filara, negocjacje w sprawie ogólnej umowy o ochronie danych między UE a USA dotyczącej danych związanych z egzekwowaniem prawa, wymiana danych PNR z państwami trzecimi, inteligentne granice, czy kwestie dotyczące współpracy wymiarów sprawiedliwości).

Kolejną bardzo ważną kwestią strategiczną przyjętą w omawianym dokumencie, było zobowiązanie GR Art. 29 do podjęcia działań, które wpłyną na poprawę jej skuteczności, co w obliczu postępującej globalizacji i przekazywania danych na szczeblu międzynarodowym nabiera szczególnego znaczenia. W Programie prac wymienia się działania normalizacyjne typu ISO, CEN, adekwatność państw trzecich, wiążące reguły korporacyjne (usprawnienie obecnych procedur, w tym wzajemne uznawanie, a także opracowanie wiążących reguł korporacyjnych dla podmiotów przetwarzających), system bezpiecznej przystani „Safe Harbor” oraz ujawnianie dokumentów przed wszczęciem postępowania sądowego. Ponadto GR Art. 29 ma zacieśnić współpracę z międzynarodowymi organami ochrony danych oraz z innymi instytucjami i organizacjami zarówno w Unii Europejskiej, jak i poza nią, w tym z Radą Europy i Federalną Komisją Handlu Stanów Zjednoczonych.

Ponadto, GR Art. 29 wezwała korporację Google do wstrzymania wprowadzenia ogłoszonych przez nią zmian w polityce prywatności i upoważniła francuski organ ochrony danych (CNIL) do sprawdzenia możliwych konsekwencji tych zmian dla ochrony danych osobowych obywateli UE.

GR Art. 29 zajęła się również kwestią ochrony prywatności i danych osobowych sportowców w kontekście zwalczania dopingu. Z tego względu Grupa przesłała pismo do Komisji Europejskiej zachęcające ją do zapewnienia przestrzegania europejskich zasad dotyczących ochrony danych i prywatności w nowej wersji kodeksu Światowej Agencji Antydopingowej (WADA).

Należy również zwrócić uwagę na przyjęty przez GR Art. 29 w dniu 25 stycznia 2012 r. dokument roboczy nr 1/2002 (WP 189) w sprawie projektu *epSOS* - Smart Open Services for European Patients.

Na kolejnym 85 posiedzeniu GR Art. 29, które odbyło się w dniach 22 – 23 marca 2012 na szczególną uwagę zasługuje przyjęcie opinii nr 1/2012 o projektach reformy ochrony danych osobowych (WP 191). Zdaniem Grupy projekty te jasno określają odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe przez cały cykl życia informacji oraz harmonizują kompetencje organów nadzorczych tak, by mogły one skutecznie zapewniać i – w razie konieczności – egzekwować przestrzeganie przepisów, zarówno indywidualnie, jak i we wzajemnej współpracy. Mimo ogólnej pozytywnej oceny proponowanego rozporządzenia **Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych (ogólne**

**rozporządzenie o ochronie danych**), które ma zastąpić 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, w opinii GR Art. 29 niektóre jego zapisy wymagają wyjaśnienia i udoskonalenia. Natomiast w odniesieniu do **dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania i ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych**, Grupa zwróciła uwagę, że obecne reżimy ochrony danych w niektórych obowiązujących instrumentach oraz organach zapewniają daleko większą ochronę, niż proponuje to wspomniany dokument. Dlatego w swojej opinii stanowczo podkreśliła, że nowa dyrektywa nie może doprowadzić do obniżenia przez Państwa Członkowskie ich obecnych standardów w zakresie ochrony danych w tym sektorze i wskazała na potrzebę podjęcia większych wysiłków legislacyjnych, by zbliżyć materialne przepisy dyrektywy do przepisów zawartych w rozporządzeniu oraz zagwarantować spójność obu tekstów.

GR Art. 29 przyjęła również opinię 2/2002 w sprawie rozpoznawania twarzy w usługach on-line i usługach mobilnych (WP 192), w której przedstawiono zalecenia dotyczące dobrych praktyk mających zastosowanie wobec tej technologii. Kwestię automatycznego odczytu danych i rozpoznawania twarzy na podstawie obrazu cyfrowego poruszono także w opinii 3/2012 w sprawie rozwoju technologii biometrycznych (WP 193). W dokumencie tym stwierdza się, że technologia rozpoznawania twarzy wchodzi w zakres biometrii, ponieważ w wielu wypadkach wskazuje szczegóły wystarczające do precyzyjnej identyfikacji danej osoby. O ile dane biometryczne danej osoby można usunąć lub zmienić, to jednak źródła, z którego pochodzą, nie da się zasadniczo zmienić ani usunąć. Stąd technologie biometryczne wymagają szczególnej uwagi ze strony Grupy Roboczej Art. 29, ponieważ ich stosowanie niesie ze sobą szereg obaw związanych z ochroną prywatności.

W dniach 6-7 czerwca 2012 r. odbyło się 86 posiedzenie GR Art. 29, na którym przyjęto opinię 4/2012 w sprawie wyjątków w zakresie pozyskiwania zgody na zapisywanie plików cookie (WP 194). W opinii omówiono rodzaje plików cookie, które pod określonymi warunkami można umieszczać na urządzeniu końcowym użytkownika bez wymogu uzyskania jego świadomej zgody. Opinia zawiera także wytyczne w zakresie podejmowania decyzji, czy określony plik cookie jest zwolniony czy też nie, z zasady pozyskania świadomej zgody przed jego umieszczeniem na terminalu użytkownika lub abonenta oraz podkreśla konieczność sprawdzenia, czy spełnione zostało jedno z kryteriów wyłączeń określonych w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. W przypadku wątpliwości operatorzy strony internetowej mogą zawsze poprosić o zgodę użytkownika, unikając w ten sposób jakiegokolwiek niepewności prawnej. GR Art. 29 przyjęła również dokument roboczy nr 2/2012 w sprawie wiążących reguł korporacyjnych dla przetwarzających (WP 195). W dokumencie

tym GR Art. 29 przedstawiła listę kontrolną opisującą warunki, które należy spełnić w celu ułatwienia wykorzystywania WRK dla przetwarzających. W liście kontrolnej określono, co powinny zawierać wiążące reguły korporacyjne oraz co należy przedstawić organowi ochrony danych we wniosku o zatwierdzenie wiążących reguł korporacyjnych. Podobne wytyczne już istnieją dla WRK dla administratorów (WP 153). W późniejszym terminie zostały również przyjęte zalecenia nr 1/2002 (WP 195a) w sprawie standardowego formularza dotyczącego WRK dla przetwarzających, który ma być wnoszony do organów ochrony danych w celu zatwierdzenia ww. wiążących reguł korporacyjnych.

Przed kolejnym 87 posiedzeniem plenarnym GR Art. 29 w swojej opinii nr 5/2012 na temat przetwarzania danych w chmurze obliczeniowej (WP 196) poddała analizie wszystkie kwestie z zakresu ochrony danych osobowych istotne dla administratorów danych i dostawców usług przetwarzania danych w chmurze w Europejskim Obszarze Gospodarczym oraz ich klientów. Jednym z kluczowych wniosków wynikających z tej opinii jest zobowiązanie podmiotów korzystających z usługi przetwarzania w chmurze, do dokonywania wnikliwej analizy potencjalnych zagrożeń. Wszyscy dostawcy usług w chmurze oferujący usługi w EOG powinni zapewnić klientowi informacje niezbędne do odpowiedniego oszacowania argumentów za i przeciw korzystaniu z takiej usługi. Bezpieczeństwo, przejrzystość i pewność prawna powinny być kluczowymi czynnikami związanymi z oferowaniem usług przetwarzania w chmurze. GR Art. 29 w kolejnych opiniach wypowiedziała się także w sprawie projektu decyzji Komisji Europejskiej dotyczącego środków mających zastosowanie do zgłaszania naruszeń ochrony danych osobowych na mocy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej (WP 197) oraz w sprawie zapewnienia odpowiedniego poziomu ochrony danych osobowych w Księstwie Monaco (WP 198)

Na 87 posiedzeniu GR Art. 29 spotkała się z posłami sprawozdawcami, którzy są odpowiedzialni za wnioski dotyczące reformy ochrony danych osobowych z ramienia Parlamentu Europejskiego, a także rozpoczęła dyskusję w sprawie aplikacji mobilnych oraz zapoznała się z pracami projektu poświęconego wdrażaniu zasady rozliczalności.

W związku z toczącymi się pracami legislacyjnymi w sprawie nowych ram prawnych ochrony danych osobowych w UE w opinii 8/2012 z dnia 5 października 2012 r. przedstawione zostały dalsze uwagi dotyczące dyskusji na temat reformy ochrony danych. W dokumencie tym przedstawiono wnioski zainteresowanych podmiotów w którym akcentują główne elementy reformy, wnosząc o zastosowanie podejścia pakietowego („sporządzenie dwóch w pełni spójnych, harmonijnych i wysokiej jakości instrumentów prawnych dotyczących ochrony danych poprzez zastosowanie kompleksowych, zrównoważonych, skoordynowanych i równoległych procedur dla obu tekstów”) oraz identyfikują szereg obszarów, które wymagają dalszej dyskusji i wyjaśnienia. Na uwagę zasługuje przedstawione w tej opinii stanowisko GR Art. 29 w odniesieniu do niektórych kluczowych pojęć w zakresie ochrony danych (definicja danych osobowych oraz pojęcie zgody) i jej sugestie sięgnięcia do niekiedy bardziej

odpowiednich rozwiązań alternatywnych. Grupa uważa, że w celu zapewnienia należytej ochrony prywatności i danych osobowych oraz aktualności rozporządzenia w przyszłości, należy przyjąć szeroką definicję danych osobowych oraz dopilnować, aby w przypadkach, w których wymagana jest zgoda, była to zgoda udzielona według wysokich standardów. W opinii GR Art. 29, jeżeli przyjęcie tych kluczowych pojęć prowadzi do nieproporcjonalnych wyników w stosowaniu przepisów rozporządzenia regulujących przetwarzanie i ustalanie praw indywidualnych, uwagę należy skupić na tych właśnie przepisach i wyjątkach od nich, nie zaś na samych pojęciach.

Na kolejnym 88 posiedzeniu plenarnym WP Art. 29 zajmowała się m.in. kwestiami związanymi z przyszłymi ramami prawnymi ochrony danych osobowych oraz aplikacjami mobilnymi.

GIODO oraz jego przedstawiciele oprócz uczestnictwa w posiedzeniach plenarnych WP Art. 29 brali również udział w pracach różnych podgrup powstałych w ramach Grupy Roboczej Art. 29, jak np. Podgrupy ds. Wiążących Reguł Korporacyjnych (WRK ang. BCR), ds. Technologii, ds. Kluczowych Postanowień Dyrektywy, ds. E-administracji i Biometrii, ds. Przyszłości Prywatności, czy nowopowstałej Podgrupy ds. Granic, Podróży i Egzekwowania Prawa. Podstawowym zadaniem wspomnianych podgrup jest dokonywanie analizy szczegółowych zagadnień dotyczących ochrony danych osobowych w wybranym obszarze oraz przygotowywania dokumentów na posiedzenia plenarne. Wynikiem prac prowadzonych przez wspomniane podmioty było przyjęcie przez GR Art. 29 opinii w sprawach, które były przedmiotem ich spotkań.

I tak dla przykładu odniesieniu do prac w ramach Podgrupy ds. E-administracji i Biometrii, przedstawiciel GIODO wniósł znaczący wkład w utworzenie precyzyjnej definicji danych biometrycznych. W kontekście możliwych zastosowań technologii biometrycznych należało bowiem uznać, że nie tylko cechy biologiczne i zachowania przypisane osobie fizycznej, ale także ich odzwierciedlenie w postaci śladów i zapisów – w szczególności w formie elektronicznej – należy uznać za dane biometryczne. Uzasadnieniem rozszerzenia tej definicji były często pojawiające się wątpliwości, czy np. zdjęcie linii papilarnych palca jest daną biometryczną, czy tylko zwykłym obrazem, lub czy np. przetworzony do postaci wektora liczb obraz linii papilarnych palca (tzw. template) jest dalej daną biometryczną czy już nie, chociażby z tego względu, że na jego podstawie nie jest możliwe odtworzenie pełnych informacji biometrycznych w postaci obrazu linii papilarnych, które były podstawą jego wytworzenia. Drugą wątpliwością, jaka się w tym kontekście pojawiła, była kwestia dokładności danych biometrycznych. Patrząc na definicję w pierwotnie zaproponowanym brzmieniu przez dane biometryczne określano biologiczne, ruchowe lub inne cechy, typu barwa głosu, sposób wypowiedzi, itp., które nie miały przełożenia na sposób ich reprezentacji w systemach biometrycznych. W przypadku natomiast przetwarzania tych danych w systemach biometrycznych zawsze będziemy mieli do czynienia nie z pełną informacją, ale jej mniej lub bardziej doskonałym

zapisem w postaci obrazu graficznego, zapisu dźwięku, nagrania video, czy też inną postacią zapisu danych odczytywanych przez różnego rodzaju czujniki (sensory) w zależności od rodzaju danej biometrycznej, która będzie przetwarzana w systemie biometrycznym. Mając na uwadze, że w wielu systemach biometrycznych obydwie formy zapisu informacji biometrycznych mogą współistnieć, przedstawiciel GIODO przedstawił propozycję, aby do tworzonej definicji tzw. wzorca danych biometrycznych (template) dodać wyjaśnienie, że termin ten obejmuje także zapis danych biometrycznych w postaci nieprzetworzonej, na podstawie którego powstaje ww. wzorzec. Ponadto zgłoszona została potrzeba uwzględnienia takiej właściwości systemów biometrycznych, jak możliwość odnawiania cech biometrycznych poprzez użycie metody, która dla wytworzenia wzorca danych biometrycznych wykorzystuje nie tylko dane biometryczne źródła danych - które dla danej osoby są niezmiennie - ale również dodatkową zmienną, po to, aby nowy wytworzony wzorzec mógł być inny niż poprzedni, który np. został w wyniku incydentu ujawniony i ze względów bezpieczeństwa nie może być dalej wykorzystywany. Ostatecznie opisane wyżej uwagi zostały uwzględnione i zawarte w Opinii 3/2012 w sprawie osiągnięć technologii biometrycznych (WP 193) przyjętej w dniu 27 kwietnia 2012 r. przez Grupę Roboczą Art. 29.

W 2012 r. przedstawiciel GIODO uczestniczył także w posiedzeniach Podgrupy ds. Technologii. Podczas jednego z takich spotkań, które odbyło się w dniu 16 października 2012 r. w Atenach, omawiana była metoda oceny skali naruszeń bezpieczeństwa ochrony danych osobowych według koncepcji zaproponowanej wstępnie przez ENISA i Polskę. Uczestnicy tego spotkania zgodni byli co do tego, że skala naruszenia bezpieczeństwa (data breach severity) powinna być zdefiniowana jako szacunkowe wyliczenie wielkości potencjału szkodliwego wpływu na prywatność osoby, której dane dotyczą oraz na ochronę tych danych. Potencjalne uderzenie w prywatność jest skutkiem naruszenia ochrony danych, np. wskutek kradzieży danych, oszustwa, upokorzenia, utraty reputacji w środowisku na skutek korzystania z usług sieci publicznych, itp. Wśród czynników, które powinny być brane pod uwagę przy ocenie ogólnej skali naruszeń wymieniane były takie elementy, jak: łatwość identyfikacji danych konkretnej osoby, ocena skali wrażliwości danych, których bezpieczeństwo naruszono (tzw. krytyczność danych), a także okoliczności i rodzaj naruszenia. Wraz ze sprawozdaniem z tego spotkania przekazane zostały Komisji Europejskiej projekty w sprawie realizacji obowiązku notyfikacji naruszeń bezpieczeństwa, które następnie omawiane były na spotkaniu GR Art. 29 w dniu 18 grudnia 2012 r.

Natomiast na posiedzeniu Podgrupy ds. Kluczowych Postanowień Dyrektywy, która odbyła się 11 maja 2012 r. z udziałem przedstawiciela GIODO, przedmiotem dyskusji było zagadnienie zgodności celu przetwarzania, celów powiązanych ze sobą, celów niezgodnych, ale uzasadnionych, sposobów identyfikacji celów, itp. Wskazywano przy tym, że często nie przywiązuje się większej wagi do zmiany

celu, jeśli istnieje podstawa prawna. Dlatego podczas obrad dobitnie podkreślono, że ochrona danych osobowych powinna opierać na dwóch kluczach: podstawie prawnej oraz zgodności z celem pierwotnym. W odniesieniu do kwestii identyfikacji celu, większość państw w przeważającej mierze opiera się na notyfikacji. Przedstawiciel polskiego organu ds. ochrony danych również wskazał na ten element zaznaczając przy tym, że ma to w dużej mierze deklarowany charakter. Faktyczne ustalenie celu może się odbyć w toku inspekcji przeprowadzanej przez GIODO lub w związku z rozpatrywaniem skarg. Najpierw należałoby jednak doprecyzować zakres, to znaczy dokonać pewnej interpretacji zgodności celu z podstawą prawną oraz wprowadzić do istniejącego formalnego podziału „zgodny” - „niezgodny” kategorię „incydentalnego” oraz „strukturalnego” wykorzystania danych.

W 2012 r. przedstawiciel GIODO w ramach Podgrupy ds. Granic, Podróży i Egzekwowania Prawa koordynował dyskusję dotyczącą wykorzystywania przez władze państw trzecich danych dotyczących pasażerów linii lotniczych (danych API).

Generalny Inspektor Ochrony Danych Osobowych, jako przedstawiciel Grupy Roboczej Art. 29, uczestniczy w przedsięwzięciach organizowanych przez różne podmioty, służąc wiedzą ekspercką na tematy związane z ochroną danych osobowych i prawem do prywatności. Przykładem może być Spotkanie Europejskiego Forum ds. e-Fakturowania (European Multi-Stakeholder Forum on e-Invoicing), które odbyło się 26 września 2012 r. w Brukseli. Było to już drugie spotkanie tego Forum z udziałem polskiego organu ds. ochrony danych osobowych.

W odniesieniu do współpracy międzynarodowej na podkreślenie zasługuje także aktywny udział Generalnego Inspektora Ochrony Danych Osobowych i jego przedstawicieli w spotkaniach organizowanych przez Europejską Agencję Bezpieczeństwa Informacji i Sieci (ENISA).

Należy również zwrócić uwagę na udział przedstawiciela GIODO w 24. warsztatach rozpatrywania spraw, zorganizowanych przez węgierski organ ochrony danych w dniach 3 - 4 września 2012 r. w Budapeszcie.

Przedstawiciel GIODO był również mówcą na trzech międzynarodowych warsztatach KE, które we współpracy z Macedońską Agencją Ochrony Danych Osobowych odbyły się w Skopje. Jeden z warsztatów (Skopje, 09-10.05.2012) poświęcony był dostępowi do orzeczeń sądowych, prawie do anonimowości i ochronie danych osobowych, podczas którego przedstawiony został materiał na temat dostępu do orzeczeń sądowych w Polsce w kontekście ochrony danych osobowych i przejrzystości działania władzy sądowniczej, a także koncepcja działania sądownictwa w świetle projektu nowych ram prawnych ochrony danych osobowych w UE. Podczas warsztatu na temat ochrony prywatności konsumentów w Internecie (Skopje, 14-15.05.2012) przedstawiciel GIODO przedstawił prezentację poświęconą zagadnieniom prywatności w fazie projektowania, prywatności w ustawieniach domyślnych, kwestii oceny wpływu na prywatność oraz ochrony danych osobowych w kontekście profilowania. Natomiast w trakcie warsztatu dotyczącego ochrony danych osobowych w związku z

planowanych transferem do państw trzecich (Skopje, 03.12.2012), przedstawił zasady przekazywania danych do państw spoza EOG oraz omówił procedurę uznawania przez KE, że dane państwo zapewnia odpowiedni poziom ochrony danych. Wydarzenia to zorganizowane było przez Dyрекcję ds. Rozszerzenia Komisji Europejskiej w ramach TAIEX (Technical Assistance and Information Office), w którym przedstawiciel GIODO brał udział – jako ekspert krajowy – przygotowujący wystąpienia tematyczne.

Na uwagę zasługuje również projekt Konsorcjum Privacy Impact Assessment Framework (PIAF) – Ramy Oceny Wpływu na Prywatność, w ramach którego zorganizowany został w Polsce warsztat poświęcony omówieniu wyników badań ankietowych skierowanych do organów ochrony danych w UE, na temat oceny wpływu na prywatność.

Przedstawiciel GIODO uczestniczył w cyklicznie organizowanych w Kijowie seminariach Rady Europy poświęconych ochronie danych osobowych w działalności mediów na Ukrainie, organizowanych w ramach projektu promującego europejskie standardy w tej dziedzinie. Jednym z celów tego projektu było wypracowanie przez środowiska dziennikarskie – przy merytorycznym wsparciu ekspertów RE – kodeksu dobrych praktyk, jako wytycznych w sprawach ochrony prywatności.

W dniu 27 czerwca 2012 r. przedstawiciel GIODO brał udział w konferencji zorganizowanej w Brukseli przez Komisję Europejską w ramach konsultacji nad projektem dotyczącym e-Justice i wystąpił w sesji poświęconej ochronie danych, przedstawiając doświadczenia polskiego organu ochrony danych w tej kwestii. Podczas kilku toczących się równolegle sesji omówiono zakres oddziaływania tego projektu i szeroki kontekst jego zastosowań, a także kwestie związane z jego zarządzaniem i zapewnieniem skutecznej ochrony danych osobowych. Europejska Strategia e-Sprawiedliwości znajduje się w obszerze szczególnej uwagi Europejskiego Inspektora Ochrony Danych Osobowych (EIOD), dla którego wymiana informacji poprzez tworzenie systemów informacji i dostępu do nich, zwłaszcza w odniesieniu do pakietu KE w zakresie zarządzania granicami Unii Europejskiej, transatlantycka wymiana informacji w celach egzekwowania prawa, ochrona dzieci korzystających z Internetu czy System Informacyjny Rynku Wewnętrznego, może stwarzać określone zagrożenia dla praw i wolności osób, których dane osobowe będą przetwarzane w tych systemach – dlatego ich zakres i cel przetwarzania podlegają wstępnej kontroli Europejskiego Inspektora Ochrony Danych.

Oprócz przedstawionej powyżej działalności Generalnego Inspektora Ochrony Danych Osobowych na polu międzynarodowym, inną formą jego aktywności był udział w różnego rodzaju krajowych i 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 różnych spotkaniach



z organami państw członkowskich UE oraz z innymi zainteresowanymi stronami zarówno w Polsce, jak i za granicą.

W ramach współpracy z organami administracji rządowej, w tym przede wszystkim z Ministerstwem Spraw Wewnętrznych i Ministerstwem Administracji i Cyfryzacji, oraz w związku z rozpoczęciem w 2012 r. wspomnianych prac nad projektami aktów ustawodawczych w zakresie ochrony danych osobowych w Unii Europejskiej, nastąpiła intensyfikacja prac Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX), w której aktywnie uczestniczył Generalny Inspektor Ochrony Danych Osobowych, udzielając polskiej delegacji merytorycznego wsparcia.

W Parlamencie Europejskim 9 i 10 października 2012 r. miało miejsce międzyparlamentarne posiedzenie komisji parlamentów narodowych ws. reformy unijnych przepisów o ochronie danych osobowych (LIBE), w którym uczestniczył Generalny Inspektor Ochrony Danych Osobowych. Dyskutowano tu nad najważniejszymi elementami reformy unijnych przepisów w zakresie ochrony danych osobowych, której założenia Komisja Europejska zaprezentowała 25 stycznia 2012 r. w Brukseli – zastąpienie unijnej dyrektywy o ochronie danych osobowych ogólnym rozporządzeniem, zaś zasady ochrony danych osobowych w sektorze policji i wymiaru sprawiedliwości będzie określała dyrektywa.

Dwudniowe spotkanie posłów do Parlamentu Europejskiego i do parlamentów państw członkowskich zostało podzielone na siedem sesji odzwierciedlających główne zagadnienia zawarte w przedstawionych przez Komisję Europejską wnioskach legislacyjnych: reforma ram prawnych UE dotyczących ochrony danych, prawo do ochrony danych, ochrona danych a egzekwowanie prawa, podmioty przetwarzające dane i administratorzy danych w sektorze prywatnym, organy ds. ochrony danych a spójność, wymiana danych przez organy policji i dostęp do prywatnych baz danych oraz ochrona danych w środowisku globalnym. W drugim dniu obrad podczas sesji „Wymiana danych przez organy policji i dostęp do prywatnych baz danych”, wystąpił dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych (GIODO), który jako jeden z dwóch przedstawicieli organów ochrony danych osobowych został poproszony o zabranie głosu.

W 2012 r. Generalny Inspektor Ochrony Danych Osobowych uczestniczył również w badaniu w oparciu o kwestionariusz jakościowy i ilościowy dotyczący zasobów organów ochrony danych, nadesłany przez Komisję Europejską, a także w badaniu przeprowadzonym przez Agencję Praw Podstawowych (APP)<sup>243</sup>, która chciała zapoznać się z opiniami swoich partnerów, w związku

---

<sup>243</sup> Agencja Praw Podstawowych Unii Europejskiej (*The European Union Agency for Fundamental Rights – FRA*), została ustanowiona na mocy rozporządzenia Rady (WE) nr 168/2007 z dnia 15 lutego 2007 r. Funkcjonuje od 1 marca 2007 r. Celem działalności Agencji jest dostarczanie instytucjom UE oraz państwom członkowskim, pomocy i wiedzy fachowej w zakresie praw podstawowych przy wdrażaniu prawa wspólnotowego.

z przygotowaniem do opracowania programu prac Agencji na 2013 rok. Celem tych badań było ustalenie, czy wskazane w kwestionariuszu dziedziny aktywności i bloki tematyczne zostały poprawnie zidentyfikowane przez Agencję oraz czy należą one do priorytetowych obszarów zainteresowania państw członkowskich.

Wymienione w kwestionariuszu działania zostały określone do czterech głównych rozdziałów: Wolność, Równość, Sprawiedliwość oraz Działania o ogólnym charakterze. Każdy z rozdziałów zawierał kilka szczegółowych zagadnień i wymieniał projekty zaplanowane przez Agencję na 2013 rok oraz ich przewidywane rezultaty. Projekty obejmują w przeważającej części działania związane z gromadzeniem danych, analizowaniem informacji, prowadzeniem badań czy opracowywaniem metod monitorowania sytuacji praw podstawowych w UE. W rozdziale „Wolność” ujęte zostały przede wszystkim działania związane z migracją (zarządzanie granicami, polityka azylowa, wykorzystywanie migrantów na rynku pracy, itd.). Aktywność APP będzie przebiegać w tym obszarze we współpracy z Europolem, Frontexem oraz Europejskim Urzędem Wsparcia w dziedzinie Azylu. Drugim z głównych zagadnień we ww. rozdziale była tematyka związana z ochroną danych osobowych. Agencja planuje utworzenie bazy danych zawierającej orzecznictwo sądów krajowych i międzynarodowych w sprawach związanych z ochroną danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych przygotował ponadto informację dla APP dotyczącą wykorzystania zadań Agencji w działalności organu ds. ochrony danych osobowych w Polsce, niezbędnych do opracowania raportu na potrzeby 12. Spotkania Krajowych Oficerów Łącznikowych przy APP UE, które odbyło się w dniach 11-12 października 2012 r. w Wiedniu.

W działalności międzynarodowej Generalnego Inspektora należy również wyróżnić udzielanie przez niego odpowiedzi na napływające z zagranicy pytania dotyczące interpretacji i stosowania przepisów polskiego prawa o ochronie danych osobowych. W przypadku organów ochrony danych pytania dotyczyły zwykle tego, jak konkretna kwestia dotycząca ochrony danych byłaby potraktowana w naszym państwie, to jest o regulacje prawne obowiązujące w danym obszarze, które stosuje się w naszym kraju. Tematem, który pojawiał się najczęściej był szeroko rozumiany monitoring. W odpowiedziach Generalny Inspektor wskazał, że w Polsce nie istnieją jednolite uregulowania w tym zakresie. Odnosząc się jednakże konkretnie do kwestii przetwarzania danych biometrycznych pracowników w celu sprawdzenia ich obecności w pracy, wskazał że takie działanie jest niedopuszczalne, nawet w przypadku wyrażenie przez nich na to zgody.

Innymi tematami, które pojawiały się w pytaniach były m.in. ochrona danych w kontekście danych klinicznych, prawa internetowego (m.in. niezamówiona informacja handlowa) czy kwestii przekazywania tzw. danych API danych dotyczących pasażerów lotniczych).

## 8.1. 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. 8).

Pierwszym w kolejności międzynarodowym wydarzeniem 2012 roku z udziałem dra Wojciecha R. Wiewiórowskiego, GIODO, były - opisane w innej części niniejszego Sprawozdania - uroczystości związane z obchodami **VI Europejskiego Dnia Ochrony Danych Osobowych, które rozpoczęły się w Brukseli w dniach 24-25 stycznia 2012 r.** W trakcie obchodów tego święta Generalny Inspektor Ochrony Danych Osobowych spotkał się z posłami do Parlamentu Europejskiego, wziął udział w 5. Międzynarodowej Konferencji pt. „Computers, Privacy and Data Protection” oraz zorganizował uroczyste spotkanie ekspertów ochrony danych osobowych z przedstawicielami Parlamentu Europejskiego, Rady Europy, Komisji Europejskiej, polskich ministerstw, urzędów centralnych i placówek dyplomatycznych w Brukseli oraz innych polskich i unijnych instytucji.

Zastrzeżenia GIODO do konwencji ACTA oraz reforma unijnych przepisów dotyczących ochrony danych osobowych były głównymi tematami tego spotkania, które odbyło się w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej przy Unii Europejskiej. Wspomniana reforma stanowi między innymi odpowiedź na postęp cywilizacyjny i gwałtowny rozwój nowoczesnych technologii. Omówienie tych kwestii było istotne m.in. dlatego, że zapowiadane zmiany w unijnych regulacjach mogą mieć wręcz rewolucyjny charakter, toteż potrzebny był aktywny udział Polski w pracach legislacyjnych na poziomie UE, w tym również Parlamentu Europejskiego. Podobne zainteresowanie wśród polskich europosłów wywołała też sprawa zastrzeżeń GIODO do konwencji ACTA, nad którą Parlament Europejski wkrótce miał rozpocząć debatę.

Natomast podczas 5. Międzynarodowej Konferencji „Computers, Privacy and Data Protection (CPDP) 2012. European Data Protection: Coming Of Age” zorganizowanej przez Vrije Universiteit Brussel (Research group on Law, Science, Technology and Society LSTS), Facultés Universitaires de Namur (Centre de Recherches Informatique et Droit CRID), Institut National de Recherche en Informatique et en Automatique INRIA, Tilburg University (Tilburg Institute for Law, Technology, and Society TILT) oraz Fraunhofer Institut für System- und Innovationsforschung ISI, Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Behavioural Biometrics in the Smart House. What does the house know about the user and what the user knows about the house” w ramach sesji „Privacy and Data Protection in Smart Grids”.

Wśród innych wydarzeń o charakterze międzynarodowym znalazły się:

1. **Międzynarodowa Konferencja „Rewizja przepisów dyrektywy o ochronie danych UE”** (Cambridge, 19-20 kwietnia 2012 r.)

Na Wydziale Prawa Uniwersytetu w Cambridge odbyła się Międzynarodowa Konferencja poświęcona nowym regulacjom prawa ochrony danych osobowych w Unii Europejskiej, podczas której Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład pt. „Prawo o ochronie danych UE a kraje trzecie”. Organizatorem tego wydarzenia był Centre for European Legal Studies (CELS).

2. **II Warsztaty „Privacy Impact Assessment Framework for Europe”** (Sopot, 24 kwietnia 2012)  
Podczas tego Spotkania Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Privacy Impact Assessment. From Philosophy to Legal Reality”, w którym przedstawił praktyczne aspekty zasady wpływu prywatności na ochronę danych osobowych. Organizatorem tego wydarzenia byli: Research Group on Law Science Technology & Society (Vrije Universiteit Brussel) oraz stowarzyszenie Privacy International.

3. **Wiosenna Konferencja Europejskich Rzeczników Ochrony Danych** (Luksemburg, 3-4 maja 2012 r.)

Wiosenna Konferencja Rzeczników Ochrony Danych 2012 odbywała się pod hasłem „Sprostać oczekiwaniom? Nowe ramy prawne ochrony danych Unii Europejskiej”. Podczas konferencji GODO wygłosił wykład pt. „Nowe ujednolicone przepisy dla wspólnego obszaru policji i wymiaru sprawiedliwości”, poświęcony praktycznym aspektom wdrożenia zasad zaproponowanych przez Komisję Europejską w przedstawionym w styczniu 2012 r. projekcie dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania i ścigania przestępstw lub wykonywania sankcji karnych oraz swobodnego przepływu tych danych. Podczas tego wydarzenia Europejscy Rzecznicy Ochrony Danych przyjęli Rezolucję w sprawie europejskiej reformy ochrony danych.

4. **Konferencja „Europejski Dzień Ochrony Danych 2012”** (Berlin, 7 maja 2012 r.)

Generalny Inspektor Ochrony Danych Osobowych wziął udział w zorganizowanej przez EUROFORUM w Berlinie, Konferencji „Europejski Dzień Ochrony Danych 2012”. Wydarzenie to odbywało się w ramach „13. Kongresu Ochrony Danych”. Podczas konferencji wygłosił wykład pt. „Czy ujednolicona ochrona danych w Europie wymaga wspólnych praktyk w zakresie egzekwowania prawa? Perspektywa Europy Środkowej i Wschodniej”.

5. **3. Coroczne Sympozjum Agencji Praw Podstawowych** (Wiedeń, 10 maja 2012 r.)

3. Coroczne Sympozjum Agencji Praw Podstawowych odbywało się pod hasłem „Reforma ochrony danych UE: nowe gwarancje praw podstawowych”. W wydarzeniu udział wzięli kluczowi eksperci z krajowych organów rządowych, organizacji międzynarodowych i pozarządowych, jak również krajowych organów ochrony danych. Wśród poruszanych tematów znalazły się następujące kwestie: prawo do bycia zapomnianym i prawo do przenoszenia danych; niezależność i uprawnienia niezależnych organów nadzorczych oraz cele, rodzaje i zabezpieczenia technik profilowania. Podczas

Seminarium dr Wojciech R. Wiewiórowski, GODO, wygłosił wystąpienie pt. „Prawo do bycia zapomnianym. Podstawowe prawo osoby oraz niebezpieczeństwo powstania *Ministerstwa Prawdy*”.

#### **6. Konferencja „Réunion internationale sur l'application de la loi” oraz Spotkanie Grupy Roboczej utworzonej w Mexico City (Montreal, 14-15 maja 2012 r.)**

Podczas spotkania przedstawiono raport z postępu prac Grupy Roboczej utworzonej w Mexico City oraz Grupy Roboczej Koordynującej GPEN<sup>244</sup>. Podczas dyskusji przedstawiono bariery i wyzwania w obszarze wymiany doświadczeń i koordynacji wspólnych działań. Omówione też zostały kwestie zmiany polityki prywatności Google, zgłaszania transgranicznych naruszeń ochrony danych, inicjatywy legislacyjne w zakresie polityk, które mogą ułatwić współpracę i koordynację, np. projekt nowego rozporządzenia UE, amerykańska „Biała Księga” czy przegląd wytycznych OECD. Podczas Spotkania Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład „Improving Practical and Helpful Co-operation between Data Protection Authorities”. Organizatorem był Spotkania był Kanadyjski Rzecznik Ochrony Prywatności.

#### **7. 14. Spotkanie Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej - CEEDPA (Kijów, 21-22 maja 2012 r.)**

Gospodarzem tegorocznego Spotkania Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej był Krajowy Organ ds. Ochrony Danych Ukrainy. Wśród uczestników spotkania znaleźli się przedstawiciele organów ochrony danych z Polski, Ukrainy, Republiki Czeskiej, Serbii, Macedonii, Słowenii, Estonii, Czarnogóry, Rosji, Węgier, Mołdawii, Bułgarii i Albanii. W wydarzeniu uczestniczył dr Wojciech Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, który wygłosił wystąpienie na temat nowych ram prawnych ochrony danych Unii Europejskiej. W trakcie Spotkania przyjęto dwie deklaracje. Pierwszą z nich była Deklaracja w sprawie nowych członków Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, na mocy której w poczet członków Grupy przyjęto organy ochrony danych z Bośni i Hercegowiny oraz Czarnogóry. W drugiej deklaracji Rzecznicy Organów Ochrony Danych Państw Europy Środkowej i Wschodniej wyrazili poparcie dla europejskiej reformy ochrony danych. Została podjęta również decyzja, że 15. spotkanie CEEDPA odbędzie się w 2013 r. w Serbii, zaś 16. zostanie zorganizowane w 2014 r. w Macedonii.

#### **8. Międzynarodowa Konferencja „Modernizacja przepisów o ochronie danych w Europie (Skopje, 30-31 maja 2012 r.)**

Generalny Inspektor Ochrony Danych Osobowych, dr Wojciech Rafał Wiewiórowski, uczestniczył w Międzynarodowej Konferencji „Modernizacja przepisów o ochronie danych w Europie” zorganizowanej przez Dyrektoriat Ochrony Danych Osobowych Macedonii w ramach projektu

---

<sup>244</sup> GPEN – Światowa Sieć Egzekwowania Przepisów o Ochronie Prywatności (Global Privacy Enforcement Network – GPEN), której GODO jest członkiem od listopada 2010 r. zob. <http://www.gido.gov.pl/1520099/j/pl/>

finansowanego przez UE „Wsparcie dla Dyrektoriatu Ochrony Danych Osobowych”, podczas której wygłosił wykład pt. „Nowe ustawodawstwo UE i zasada oceny skutków w zakresie ochrony danych”.

9. **25. Doroczna Międzynarodowa Konferencja Privacy Laws & Business** (Cambridge, 2-4 lipca 2012 r.)

Tematem tegorocznej konferencji było „Pokonywanie przeszkód w ochronie prywatności”, która z inicjatywy Privacy Laws & Business odbyła się na Uniwersytecie w Cambridge. W konferencji uczestniczyli po raz pierwszy przedstawiciele z Brazylii i Afryki Południowej – państw, w których mają zostać przyjęte nowe regulacje dotyczące ochrony prywatności. Generalny Inspektor Ochrony Danych Osobowych wygłosił dwa referaty. Pierwszy z nich pt. „Ponowne wykorzystywanie informacji z sektora publicznego na rynku komercyjnym”, poświęcony był planowanym zmianom w dyrektywie o ponownym przetwarzaniu informacji sektora publicznego zaprezentowanych przez Komisję Europejską w ramach tzw. "Open Data Package". Drugi – „Przenoszenie mojej tożsamości cyfrowej: za i przeciw profilowaniu oraz zasady przenoszenia danych w nowych ramach prawnych ochrony danych UE” - skupił się na problematyce profilowania i możliwościach przenoszenia profili pomiędzy systemami zarządzanymi przez różnych administratorów danych osobowych. GODO wziął również udział w panelu „Interoperacyjność między Europą, obu Amerykami oraz regionem Azji i Pacyfiku. Pokonywanie różnic między systemami regionalnymi”, przedstawiając globalne aspekty nowelizacji Konwencji 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, do której miał wkrótce przystąpić Urugwaj, pierwszy kraj spoza Rady Europy.

10. **3. Konferencja poświęcona Privacy Impact Assessment Framework – PIAF** (Bruksela, 27 września 2012 r.)

Na zaproszenie Konsorcjum Privacy Impact Assessment Framework (Ramy Oceny Wpływu na Prywatność), przedstawiciele GODO uczestniczyli w 3. Konferencji poświęconej PIAF, która odbyła się 27 września 2012 r. w Brukseli. Konferencja ta stanowiła podsumowanie dwudziestomiesięcznego projektu PIAF, trwającego od stycznia 2011 r. do sierpnia 2012 r. W ramach tego przedsięwzięcia przeprowadzone zostały badania nad określeniem wpływu ram ochrony danych osobowych na prywatność, dla Dyrekcji Generalnej Komisji Europejskiej ds. Sprawiedliwości.

11. **Międzyparlamentarne posiedzenie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych** (Bruksela, 9-10 października 2012 r.)

Generalny Inspektor Ochrony Danych Osobowych uczestniczył w Międzyparlamentarnym Posiedzeniu Komisji pt. „Reforma ram prawnych UE w zakresie ochrony danych – budowanie zaufania w cyfrowym, zglobalizowanym świecie”, zorganizowanym w Parlamencie Europejskim w Brukseli, podczas którego wygłosił referat pt. „Police data sharing and access to private data bases”. Międzyparlamentarne posiedzenie przygotowywane było wspólnie przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) oraz Dział ds. Dialogu

Ustawodawczego. Podstawowym celem tego przedsięwzięcia było wskazanie i omówienie niektórych z najważniejszych kwestii dotyczących nowych ram ochrony danych i zaangażowanie posłów do Parlamentu Europejskiego i do parlamentów państw członkowskich, w wymianę poglądów i konstruktywny dialog. Taki dialog ma podstawowe znaczenie, ponieważ już kilka parlamentów państw członkowskich wyraziło zainteresowanie proponowanymi aktami prawnymi, co widać było w kilku uzasadnionych opiniach i dokumentach przekazanych przez parlamenty krajowe. W posiedzeniu wzięło udział kilku przedstawicieli Polskiego Parlamentu, z którymi GIODO zamierza zorganizować wiosną 2013 roku spotkanie poświęcone analizie praktycznego wpływu ogólnego rozporządzenia o ochronie danych na ustawodawstwo państw członkowskich UE.

**12. 34. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności**  
(Punta del Ester w Urugwaju, 22-26 października 2012 r.)

Generalny Inspektor Ochrony Danych Osobowych oraz jego przedstawiciel uczestniczyli w 34. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, zorganizowanej przez Jednostkę ds. Regulacji i Kontroli Danych Osobowych (URCDP) w Punta del Este w Urugwaju. Motto tegorocznej Międzynarodowej Konferencji „Równowaga między ochroną prywatności a technologią” było punktem wyjścia do dyskusji na temat wpływu ochrony prywatności i technologii na społeczeństwo informacyjne, dane osobowe i e-administrację. Geolokalizacja, e-zdrowie, biometria, nowe przepisy UE o ochronie danych oraz wyzwania związane z piractwem i ochroną prywatności to niektóre spośród tematów, które były poruszane podczas tego wydarzenia. W czasie konferencji wystąpienia przedstawiło ponad 90. prelegentów, reprezentujących 40 krajów. Generalny Inspektor Ochrony Danych Osobowych wygłosił przemówienie w sesji poświęconej biometrii. Istotnym punktem 34 Międzynarodowej Konferencji było przyjęcie trzech dokumentów: Rezolucji o przetwarzaniu danych w chmurze obliczeniowej, Rezolucji o przyszłości prywatności oraz Urugwajskiej deklaracji w sprawie profilowania. Podczas tego wydarzenia podjęto decyzję o przyznaniu statusu organizatora kolejnej Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności polskiemu organowi ds. ochrony danych osobowych. 35. Międzynarodowa Konferencja odbędzie się w dniach 23-26 września 2013 r. w Warszawie. Międzynarodowe Konferencje to najważniejsze spotkania, w których biorą udział rzecznicy ochrony danych osobowych z Europy - na czele z Europejskim Inspektorem Ochrony Danych – i z krajów pozaeuropejskich, m.in. Kanady, USA, Australii, Hongkongu, przedstawiciele instytucji UE, rządów państw spoza UE, uznani eksperci zajmujący się tą problematyką, przedstawiciele świata akademickiego, organizacje krajowe i międzynarodowe działające na rzecz praw człowieka, jak i przedstawiciele biznesu.

**13. Seminarium dla pracowników albańskiego organu ochrony danych osobowych** (Tirana, 9 listopada 2012 r.)

Przedstawiciel GIODO był uczestnikiem seminarium dla pracowników albańskiego urzędu rzecznika ochrony danych osobowych, zorganizowanym w Tiranie w ramach projektu IPA-2009 p.t.: „Wzmocnienie Urzędu Rzecznika Ochrony Danych Osobowych w Albanii”. Podczas tego wydarzenia przedstawił prezentację poświęconą prywatności na etapie projektowania, zapewnieniu prywatności poprzez ustawienia domyślne oraz ocenie wpływu na prywatność.

**14. Warsztat „Global Interoperability: A Goal within Reach?”** (Bruksela, 13 listopada 2012 r.)

Wydarzenie to odbyło się w ramach spotkania IAPP (The International Association of Privacy Professionals), stowarzyszenia zrzeszającego praktyków z ponad 70 krajów zajmujących się tematyką ochrony prywatności. Warsztat poświęcony był problematyce wpływu harmonizacji prawa UE w zakresie ochrony danych osobowych na działalność biznesową międzynarodowych przedsiębiorstw i organizacji.

**15. III Międzynarodowa Konferencja „Ochrona Danych Osobowych”** (Moskwa, 21-22 listopada 2012 r.)

Konferencja odbyła się z inicjatywy Federalnej Służby Nadzoru w sektorze Łączności, Technologii Informacyjnych i Masowej Komunikacji Federacji Rosyjskiej. Uczestniczyli w niej przedstawiciele organów właściwych w zakresie ochrony danych osobowych z krajów Europy oraz regionu Azji i Pacyfiku. Podczas pierwszego dnia konferencji, która miała charakter okrągłego stołu, przedstawiciele zagranicznych organów oraz rosyjskiego organu ochrony danych dyskutowali na temat współpracy międzynarodowej w obszarze ochrony danych pod kątem doświadczeń krajowych. Przedstawiciel GIODO przedstawił prezentację zatytułowaną „Międzynarodowa współpraca w obszarze ochrony danych osobowych – doświadczenia krajowe”. Natomiast w drugim dniu podczas konferencyjnych sesji plenarnych prelegenci poruszyli między innymi następujące tematy: nowe regulacje dotyczące poziomów i wymogów dotyczących ochrony danych osobowych, administracyjne i międzynarodowe aspekty unijnej reformy ochrony danych czy też nakładanie kar jako najsilniejsza broń organu ochrony danych.

## **8.2. Wizyty robocze**

W działalności Generalnego Inspektora tradycyjnie dużą rolę odgrywa współpraca dwustronna, która polega m.in. na wymianie informacji, pomocy przy prowadzeniu postępowań administracyjnych i wizytach roboczych. Uzyskana pomoc niejednokrotnie przyczyniała się do zebrania materiału dowodowego niezbędnego do rozstrzygania rozpatrywanych spraw administracyjnych. Uzyskane zaś przez Generalnego Inspektora informacje o charakterze porównawczym wykorzystywane były w dalszej jego pracy.



W dniach 5-9 listopada 2012 r. z wizytą roboczą przyjechali do Polski przedstawiciele bułgarskiego organu ochrony danych osobowych – DPA. Pięciodniowa wizyta delegacji 5 przedstawicieli Bułgarskiej Komisji ds. Ochrony Danych Osobowych odbywała się w ramach projektu mobilności Leonardo da Vinci. Jej celem było umożliwienie przedstawicielom bułgarskiego i polskiego organu ochrony danych osobowych wymiany wiedzy i doświadczeń związanych z wdrażaniem prawa ochrony danych osobowych w tych dwóch krajach. W trakcie pobytu goście zapoznali się ze strukturą organizacyjną polskiego urzędu, a także z zadaniami i zakresem obowiązków realizowanych w poszczególnych departamentach Biura GIODO. Szczególnie dogłębnie omówione zostały zagadnienia związane ze współpracą międzynarodową, a także działalność edukacyjna i szkoleniowa prowadzona przez polski organ ochrony danych osobowych. Reprezentanci Bułgarskiej Komisji ds. Ochrony Danych Osobowych mieli szansę zaprezentować strukturę i działania realizowane w ramach swojego urzędu, co pozwoliło na porównanie praktyk stosowanych w tych dwóch organach ochrony danych osobowych.

### **8.3. Międzynarodowe warsztaty**

#### **a) 2. warsztaty w ramach projektu Privacy Impact Assessment Framework - PIAF (Sopot, 24 kwietnia 2012 r.)**

W ramach projektu PIAF, podmioty zrzeszone w Konsorcjum Privacy Impact Assessment Framework (Ramy Oceny Wpływu na Prywatność): Vrije Universiteit Brussel – Research Group on Law, Science, Technology & Society (VUB--LSTS), Trilateral Research & Consulting LLP oraz Privacy International, prowadziły badania dotyczące ram oceny wpływu na prywatność (PIA) dla Dyrekcji Generalnej KE ds. Sprawiedliwości. Podczas trwania projektu odbywały się warsztaty dla organów ochrony danych osobowych oraz wybranych decydentów politycznych, których celem była prezentacja wniosków z badań i poczynienie ustaleń co do działań na przyszłość. Pierwszy warsztat odbył się 12 października 2011 r. w Brukseli i poświęcony był wskazaniu najważniejszych elementów istniejących struktur PIA. Drugi warsztat zorganizowany został przez polski organ ds. ochrony danych osobowych w dniu 24 kwietnia 2012 r. w Sopocie. Praca w nim skupiała się na empirycznych badaniach czynników kontekstowych wpływających na wprowadzenie struktur PIA w państwach członkowskich UE, zgromadzonych w wyniku ankiety skierowanej do organów ochrony danych w UE<sup>245</sup>.

#### **b) Warsztaty rozpatrywania spraw (Budapeszt, 3-4 września 2012 r.)**

Pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych systematycznie uczestniczą w warsztatach rozpatrywania spraw, tzw. warsztatach skargowych (case handling workshop), które

---

<sup>245</sup> Więcej informacji nt. projektu PIAF: <http://www.piafproject.eu>

odbywają się 1-2 razy w roku z udziałem przedstawicieli organów ochrony danych osobowych działających zarówno na poziomie krajowym jak i lokalnym oraz Europejskiego Inspektora Ochrony Danych. Warsztaty mają na celu praktyczną wymianę doświadczeń pomiędzy pracownikami poszczególnych organów, którzy na co dzień zajmują się rozpatrywaniem skarg lub przeprowadzaniem inspekcji. Przedstawiciel GIODO wziął udział w 24. warsztatach rozpatrywania skarg, zorganizowanych w dniach 3-4 września 2012 r. w Budapeszcie przez węgierski organ ochrony danych osobowych.

**c) Warsztaty poświęcone dostępowi do orzeczeń sądowych, prawie do anonimowości i ochronie danych osobowych** (Skopje, 9-10 maja 2012 r.), podczas których przedstawiciel polskiego organu ds. ochrony danych osobowych wygłosił prezentację dotyczącą dostępu do orzeczeń sądowych w Polsce w kontekście transparentności i ochrony danych osobowych oraz prezentację poświęconą działalności sądów w świetle projektu nowych ram prawnych ochrony danych osobowych w Unii Europejskiej.

**d) Warsztaty dotyczące ochrony prywatności konsumentów w Internecie** (Skopje, 14-15 maja 2012 r.) - tematem wystąpienia przedstawiciela GIODO była koncepcja prywatności na etapie projektowania, prywatności w ustawieniach domyślnych i ocena wpływu na prywatność, a także zagadnienia ochrony danych osobowych w kontekście profilowania.

**e) Warsztaty ochrony danych osobowych przy przekazywaniu ich do państw trzecich** (Skopje, 3 grudnia 2012 r.), podczas których przedstawione zostały dwie prezentacje. Jedna dotyczyła zasad przekazywania danych osobowych do państw trzecich, druga zaś poświęcona była procedurze zmierzającej do uznania przez Komisję Europejską, że dane państwo trzecie zapewnia odpowiedni poziom ochrony danych osobowych. Warsztaty poświęcone ocenie odpowiedniego poziomu ochrony danych osobowych przy przekazywaniu danych do państw trzecich zostały zorganizowane przez Komisję Europejską w ramach TAIEEX. Wzięli w nich udział pracownicy macedońskiego organu ochrony danych osobowych oraz przedstawiciele organów administracji centralnej, którzy byli zaangażowani w tę procedurę

**f) Warsztat ochrony danych w badaniach farmaceutycznych** (Paryż, 3 października 2012 r.) Generalny Inspektor Ochrony Danych Osobowych uczestniczył w warsztatach pt. „Ochrona danych w badaniach farmaceutycznych i bezpieczeństwo leków: dialog między organami ochrony danych i sektorem farmaceutycznym”, zorganizowanych w Paryżu przez International Pharmaceutical Privacy Consortium – międzynarodową organizację zrzeszającą specjalistów zajmujących się ochroną danych osobowych w przedsiębiorstwach farmaceutycznych. Podczas wydarzenia GIODO brał udział

w dyskusji panelowej dotyczącej ochrony danych w procedurach monitorowania bezpieczeństwa leków po ich wprowadzeniu do obrotu

**g) Warsztat „Global Interoperability: A Goal within Reach?”** (Bruksela, 13 listopada 2012 r.)  
GIODO uczestniczył w warsztatach poświęconych problematyce wpływu harmonizacji prawa UE w zakresie ochrony danych osobowych na działalność biznesową międzynarodowych przedsiębiorstw i organizacji. Podczas tego spotkania wypowiadał się na temat potrzeby harmonizacji harmonizacji unijnego prawa ochrony danych osobowych. Spotkanie zorganizowane zostało 13 listopada 2012 r. w Brukseli w ramach spotkania IAPP (The International Association of Privacy Professionals), stowarzyszenia zrzeszającego ponad 10 000 praktyków z ponad 70 krajów zajmujących się tematyką ochrony prywatności.

### **Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2012 roku**

Generalny Inspektor Ochrony Danych Osobowych w ramach swoich kompetencji ujętych w art. 12 ustawy o ochronie danych osobowych, wykonuje szereg zadań w nim określonych, wśród których znajdują się szeroko zakrojone **działania informacyjno – edukacyjne** związane z propagowaniem idei ochrony danych osobowych i prawem do prywatności. Patronuje wielu wydarzeniom organizowanym przez inne podmioty, wpływając w ten sposób na świadomość obywateli w kwestii bezpieczeństwa dotyczących ich danych osobowych. Jest organizatorem i uczestnikiem wielu konferencji krajowych i międzynarodowych, aktywnie angażuje się w liczne działania upowszechniające wiedzę (wydawanie informacji, publikacji, broszur w zakresie ochrony danych i prywatności, wywiady i konferencje prasowe), podejmuje działania edukacyjne w formie różnych konkursów, w tym konkursów wiedzy z zakresu ochrony danych osobowych, Dni Otwartych GIODO w różnych obszarach Polski, a także organizuje bezpłatne szkolenia i warsztaty adresowane głównie do przedstawicieli administracji rządowej i samorządowej oraz przedstawicieli instytucji publicznych. Współpracuje ze szkołami wyższymi, do grona których w 2012 r. dołączyła Wyższa Szkoła Zarządzania i Bankowości w Krakowie oraz Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie. W ramach zawartych z tymi podmiotami porozumień podejmowane są różnego rodzaju inicjatywy, jak organizacja studiów podyplomowych, konferencje, debaty i seminaria promujące tematykę prywatności i ochrony danych osobowych, a także szkolenia podnoszące poziom wiedzy zawodowej i umiejętności praktyczne. Generalny Inspektor współpracuje również z różnymi organizacjami, jak np. samorządowe ośrodki doskonalenia zawodowego nauczycieli, organizacje pozarządowe oraz z takimi podmiotami, jak Polski Związek Przemysłu Motoryzacyjnego czy Państwowa Inspekcja Pracy, z którymi zawarł w 2012 r. porozumienia o współpracy.

W działalności GIODO na **arenie międzynarodowej** na podkreślenie zasługują przygotowywane odpowiedzi na pytania nadsyłane od różnych instytucji w sprawach dotyczących stanowiska polskiego organu wobec zagadnień związanych z ochroną danych osobowych, wśród których najliczniejsze stanowiły zapytania od Podgrup Grupy Roboczej Art. 29, w tym Podgrupy Technologicznej oraz Podgrupy ds. Biometrii i eGovernment. W roku 2012 wymienione podgrupy zwracały się między innymi o wypełnienie ankiet dotyczących: uwag do nowej polityki prywatności firmy Google Inc., uwag i zastrzeżeń do polityki prywatności portalu społecznościowego Facebook, w tym sformułowanych przez Grupę Roboczą Art. 29 pytań o wyjaśnienie stosowanych przez Facebook polityk prywatności, stosowanych w Polsce rozwiązań z zakresu biometrii oraz wymagań prawnych związanych z ich wprowadzaniem, np. czy wymagana jest uprzednia zgoda GIODO, podstaw prawnych oraz stosowanych procedur przy przetwarzaniu danych przez zespoły powołane do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet (CERTy), zdarzeń w zakresie naruszeń bezpieczeństwa ochrony danych i ich klasyfikacji na potrzeby oceny opracowanego przez Europejską Agencję Bezpieczeństwa Informacji i Sieci (ENISA) na zlecenie Grupy Art. 29 schematu oceny skali naruszeń bezpieczeństwa, stanu wdrożenia do prawa narodowego zaleceń znowelizowanej dyrektywy 2002/58 o E-Prywatności.

W granicach swoich kompetencji Generalny Inspektor Ochrony Danych Osobowych wydawał **opinie oraz dokonywał ustaleń co do stanów faktycznych**. Spośród wielu projektów aktów prawnych opiniowanych przez GIODO wymienić należy m.in. ustawę prawo energetyczne oraz projekty Urzędu Regulacji Energetyki w zakresie wdrażania technologii opomiarowania inteligentnego, opinie do wprowadzonych przez Ministra Edukacji zmian do projektu rozporządzeń w sprawie warunków technicznych dla sprzętu oraz oprogramowania służącego prowadzeniu lokalnych baz danych Systemu Informacji Oświatowej (SIO), warunków technicznych przekazywania i pozyskiwania danych z tej bazy oraz procedur weryfikacji dostępu do niej, a także opinię dotyczącą skutków wejścia w życie nowych przepisów w sprawie redukcji niektórych obciążeń administracyjnych w gospodarce w zakresie dotyczącym proponowanych zmian do ustawy o ochronie danych osobowych. Wypowiadał się także w odniesieniu do projektów aktów wykonawczych Ministra Spraw Wewnętrznych i Administracji w sprawie pomieszczeń przeznaczonych dla osób zatrzymanych lub doprowadzonych w celu wytrzeźwienia, pokoi przejściowych, tymczasowych pomieszczeń przejściowych i policyjnych izb dziecka oraz sposobu postępowania z zapisami obrazu z tych pomieszczeń, w sprawie projektu rozporządzenia Ministra Spraw Wewnętrznych w sprawie przetwarzania informacji, w tym danych osobowych, przez policję, a także do projektu rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej w sprawie sposobu, trybu oraz warunków technicznych gromadzenia, przetwarzania, udostępniania i usuwania przez Głównego Inspektora Transportu Drogowego utrwalonych obrazów i danych.

GIODO opracował ponadto szereg opinii do projektów rozporządzeń Ministra Zdrowia m.in. w sprawie minimalnej funkcjonalności dla systemów teleinformatycznych umożliwiających świadczeniobiorcy umawianie się na wizyty lekarskie; sposobu, trybu i terminów występowania do Narodowego Funduszu Zdrowia oraz udostępnienia przez ten podmiot świadczeniobiorcom informacji o prawie do świadczenia opieki zdrowotnej oraz o udzielonych świadczeniach; klasyfikacji danych i systemu kodów w Systemie Informacji Medycznej (SIM), a także w sprawie określenia minimalnych wymagań dla niektórych systemów teleinformatycznych funkcjonujących w ramach obsługi systemu informacji w ochronie zdrowia.

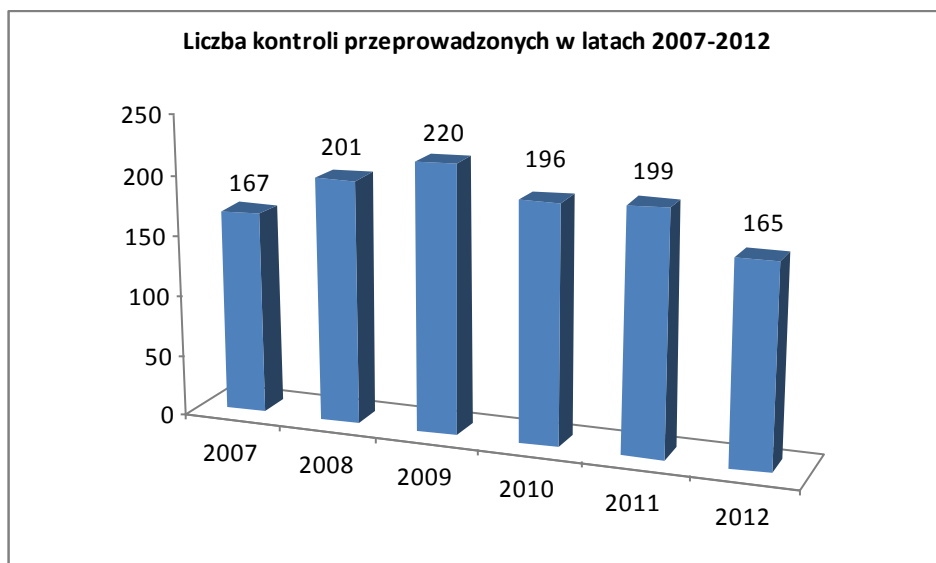
Wśród wydanych opinii do projektów rozporządzeń Ministra Zdrowia znalazły się m.in. te dotyczące opisu systemu teleinformatycznego, w którym prowadzony jest rejestr zezwoleń na prowadzenie hurtowni farmaceutycznych, aptek i punktów aptecznych oraz rejestr zgód na prowadzenie aptek szpitalnych i zakładowych, a także opis minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych.

Przedmiotem szczególnej uwagi Generalnego Inspektora Ochrony Danych Osobowych były też projekty rozporządzeń dotyczących Systemu Rejestru Usług Medycznych Narodowego Funduszu Zdrowia, Systemu Monitorowania Zagrożeń, Systemu Ewidencji Zasobów Ochrony Zdrowia, Dobrej Praktyki Klinicznej, Wspomagania Ratownictwa Medycznego, wymagań dla Systemu Informacji Medycznej, Systemu Monitorowania Kosztów Leczenia i Sytuacji Finansowo-Ekonomicznej Podmiotów Leczniczych, a także utworzenia Krajowego Rejestru Nowotworów.

W 2012 r. Generalny Inspektor Ochrony Danych Osobowych kontynuował prace merytoryczne w takich obszarach jak **monitoring i sieci inteligentne**. W zakresie monitoringu przygotowany został materiał prezentujący wkład GIODO do oczekiwanej ustawy o monitoringu wizyjnym, który został zaprezentowany podczas Międzynarodowej Konferencji „Miasto monitorowane, personel, aspekty prawne i technika systemów CCTV” współorganizowanej przez Krajową Radę Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej, która odbyła się w dniach 17-18 maja 2012 r. w Częstochowie. Tematyka monitoringu wizyjnego prezentowana była również na konferencji zorganizowanej przez Rzecznika Praw Obywatelskich i Generalnego Inspektora Ochrony Danych Osobowych pod tytułem „Kto na nas patrzy”. Innym ważnym tematem było zagadnienie **inteligentnego pomiaru** i związane z nią zagrożenia prywatności. Występujące w tym zakresie zagrożenia oraz rekomendacje dotyczące stosowania inteligentnych liczników zebrane zostały w opracowaniu zatytułowanym „Inteligentne liczniki – czy są niezbędne, w czym pomagają i jakie wątpliwości budzą ich instalacje”. Tezy zawarte w tym opracowaniu prezentowane były na konferencji „Inteligentne sieci- rynek, konsument i zasada zrównoważonego rozwoju”, zorganizowanej przez

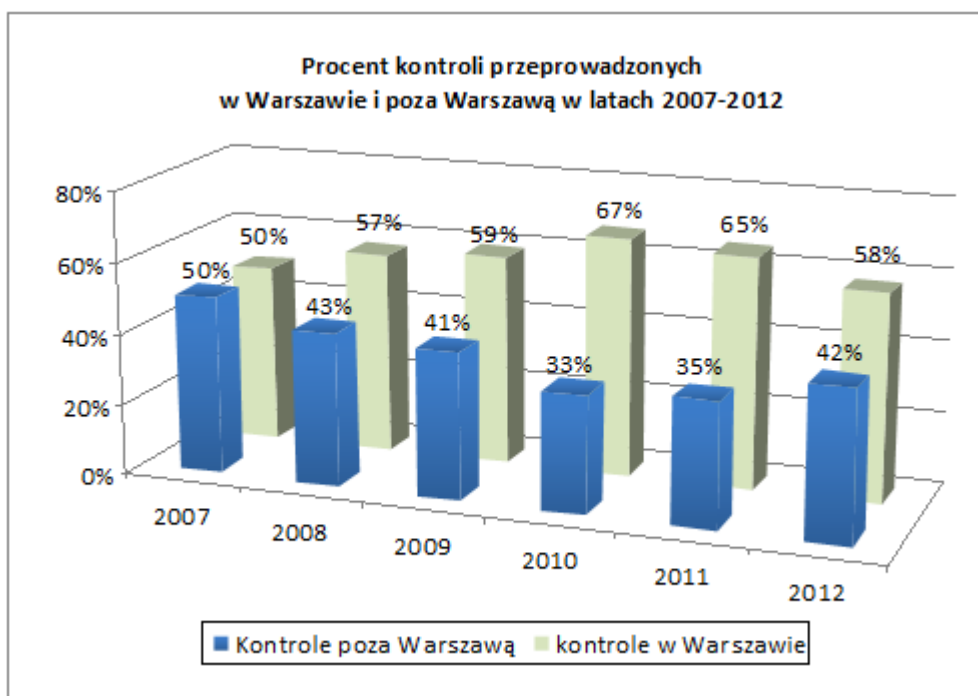
Urząd Regulacji Energetyki w dniu 18 września 2012 r. w Warszawie oraz na konferencji „II Smart Communications & Technology Forum”, zorganizowanej przez Center for Business Education w dniu 27 września 2012 r. w Gdańsku.

Natomiast charakteryzując działalność Generalnego Inspektora Ochrony Danych Osobowych w obszarze związanym z **kontrolą** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych, należy stwierdzić, że w porównaniu z rokiem 2011 liczba przeprowadzonych kontroli zmalała ze 199 do 165 (*Wykres 41*).



*Wykres 41: Porównanie liczby kontroli przeprowadzonych w latach 2007–2012.*

W analizowanym 2012 roku na ogólną liczbę 165 kontroli, 96 z nich przeprowadzonych było w Warszawie (58%), zaś 69 poza Warszawą (42%).



Wykres 42: *Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2007–2012.*

Najwięcej kontroli przeprowadzonych zostało z urzędu (92). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący.

Inicjatywa kontroli	Liczba kontroli
Z urzędu	92
Departament Orzecznictwa, Legislacji i Skarg	45
Departament Rejestracji Zbiorów Danych Osobowych	8
Departament Edukacji Społecznej i Współpracy Międzynarodowej	2
Prokuratura	1
Policja	1
Generalny Inspektor Informacji Finansowej	1
W związku z inną kontrolą	15
<b>RAZEM</b>	<b>165</b>

Czynnościom kontrolnym poddane zostały m. in. banki spółdzielcze, podmioty prowadzące hotele, dostawcy usług telekomunikacyjnych, podmioty mające dostęp do danych przetwarzanych w systemie informacji o szkolnictwie wyższym i podmioty przetwarzające dane osobowe potencjalnych dawców oraz dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej. 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.

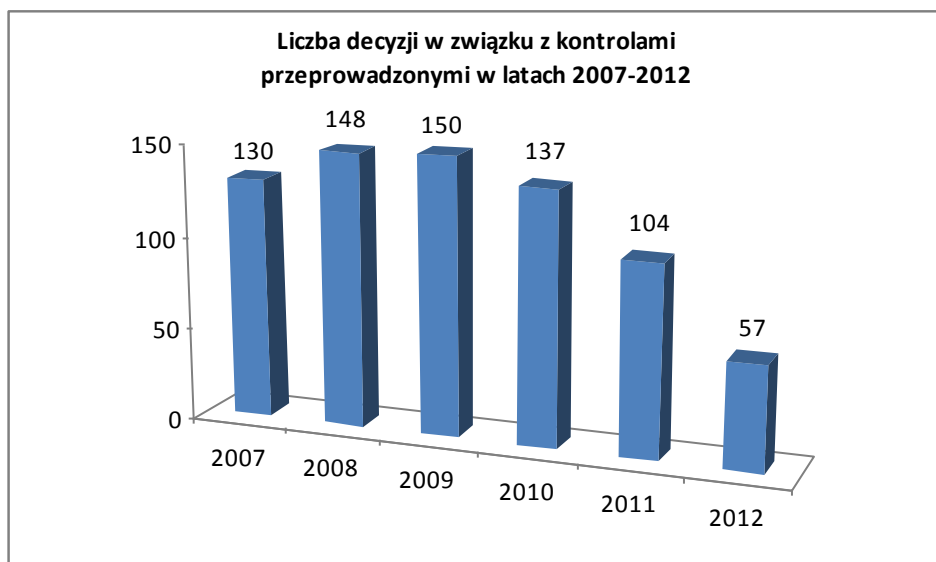
W okresie sprawozdawczym szczególny nacisk położony został na przeprowadzenie tzw. **kontroli sektorowych**, którymi objęto w 2012 r. banki spółdzielcze i banki zrzeszające banki spółdzielcze (11 kontroli), podmioty prowadzące hotele (11 kontroli), dostawców usług telekomunikacyjnych (5 kontroli), podmioty mające dostęp do danych przetwarzanych w systemie informacji o szkolnictwie wyższym (10 kontroli) oraz podmioty przetwarzające dane osobowe potencjalnych dawców oraz dawców allogenicznego szpiku i komórek krwiotwórczych krwi obwodowej (9 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 2012 r., 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. W sumie przeprowadzono 11 takich kontroli.

Ponadto w 2012 r. przeprowadzono kontrole w sądach (3 kontrole) i w jednostkach organizacyjnych prokuratury (3 kontrole) w zakresie wpisów w Systemie Informacyjnym Schengen (SIS) dokonywanych na podstawie art. 95 Konwencji Wykonawczej do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. UE z 2000 r., Nr 239, poz. 19 z późn. zm.), w związku z decyzją Wspólnego Organu Nadzorczego Schengen (WON Schengen) o przeprowadzeniu audytu tych wpisów w sposób wskazany w kwestionariuszu przygotowanym przez WON Schengen.

W 2012 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał łącznie 57 **decyzji administracyjnych**.





Wykres 43: **Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2007–2012.**

Spadek liczby decyzji wydanych w 2012 r. w porównaniu z poprzednimi latami spowodowany był m.in. mniejszą liczbą przeprowadzonych kontroli oraz znaczną poprawą stosowania przepisów o ochronie danych osobowych przez podmioty kontrolowane. Ponadto wielu administratorów danych osobowych podejmowało również działania mające na celu przywrócenie stanu zgodnego z prawem niezwłocznie po zakończeniu czynności kontrolnych.

Oceniając wyniki przeprowadzonych kontroli należy stwierdzić, że istnieje grupa administratorów danych, która miała problemy z prawidłowym wykonaniem podstawowych obowiązków określonych w przepisach o ochronie danych osobowych. Nieprawidłowości w tym zakresie dotyczyły przede wszystkim niewłaściwego dopełniania wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 i art. 25 ustawy o ochronie danych osobowych. 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.

Do dość częstych uchybień należało również niezgłaszanie prowadzonych zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi oraz zbieranie 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 zawarty w tych przepisach. Wskazać również należy na przypadki przekroczenia wynikającego z przepisów prawa, dozwolonego zakresu przetwarzanych danych, co 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 często mają także problemy z prawidłowym sformułowaniem treści oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych, tak aby wyrażona w taki sposób zgoda nie była domniemana lub dorozumiana z oświadczenia woli o innej treści. Analiza treści oświadczeń zebranych w toku kontroli niejednokrotnie wskazywała, że osobom składającym oświadczenie nie została zapewniona swoboda (możliwość 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.

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, zabranieniem 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.

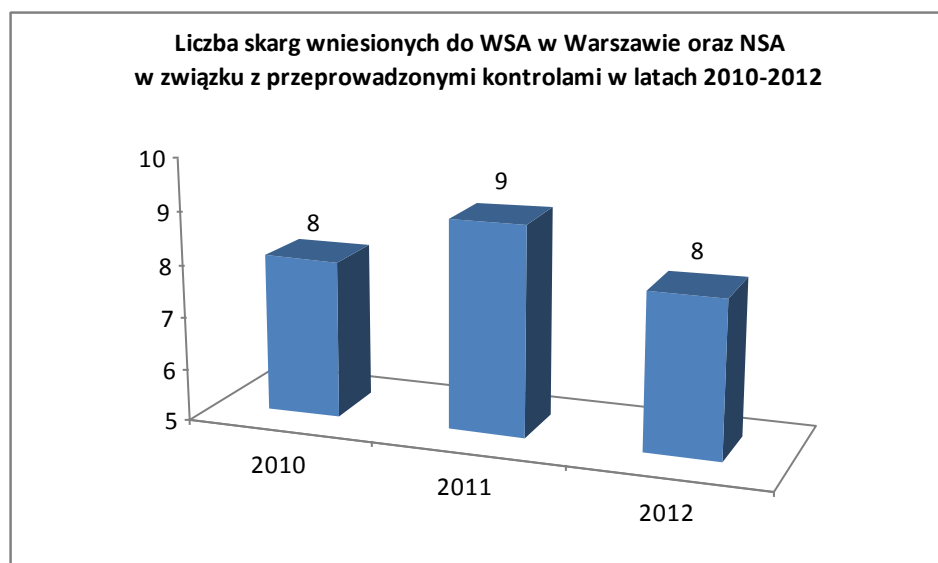
W tym miejscu należy jednak podkreślić, że urządach działających w sektorze **administracji publicznej** nastąpił zdecydowany wzrost stopnia realizacji przepisów o ochronie danych osobowych w porównaniu z wynikami za rok 2011. Oznacza to, iż w świadomości użytkowników przetwarzających dane osobowe obywateli zagadnienia dotyczące ochrony danych osobowych nabrały szczególnego znaczenia i postrzegane były jako jedno z podstawowych zadań stojących przed urzędem administracji publicznej.

Obowiązki określone w przepisach o ochronie danych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Częstą przyczyną był również, jak wskazywali administratorzy danych, brak odpowiednich środków finansowych, niezbędnych do pokrycia kosztów związanych z wdrożeniem rozwiązań zapewniających prawidłowe spełnienie wymogów. W niektórych przypadkach przyczyny powyższego

stanu rzeczy wynikały także z niewłaściwego podejścia osób odpowiedzialnych za przetwarzanie danych osobowych do problematyki ochrony tych danych, a nawet lekceważenia tych przepisów. Świadczy o tym w szczególności niewykonywanie tych obowiązków, które nie pociągają za sobą nadmiernych kosztów finansowych, np. brak ewidencji osób upoważnionych do przetwarzania danych osobowych, czy też niewyznaczenie administratora bezpieczeństwa informacji. Jednocześnie należy wskazać, że wśród jednostek poddanych w 2012 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 2012 do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego skierowanych zostało **8 skarg** w związku z przeprowadzonymi kontrolami.



Wykres 44: *Zestawienie porównawcze liczby skarg wniesionych do Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2010-2012.*

Do istotnych orzeczeń, jakie zapadły w okresie sprawozdawczym w sprawach, w których przeprowadzane były kontrole, należał wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 16 kwietnia 2012 r. (sygn. akt II SA/Wa 129/12), w którym sąd stwierdził m.in., iż umieszczenie na karcie miejskiej imienia i nazwiska oraz wizerunku jej posiadacza było wystarczające dla umożliwienia weryfikacji, czy daną kartą, jako nośnikiem imiennego biletu komunikacji miejskiej, posługuje się osoba upoważniona do jej używania. Tym samym sąd uznał, że kodowanie numeru PESEL na karcie w celu jednoznacznej identyfikacji posiadacza karty było nieadekwatne do tego celu. Sąd wskazał również, iż kodowanie numeru PESEL na karcie, jako nośniku imiennego biletu komunikacji miejskiej, w celu jej ewentualnego wykorzystania w przyszłości jako uniwersalnego narzędzia wnoszenia opłat za inne usługi miejskie, wbrew argumentacji skarżącego, narusza także zasadę adekwatności określoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych<sup>246</sup>.

Do ważnych orzeczeń sądu administracyjnego należy również postanowienie Naczelnego Sądu Administracyjnego z dnia 11 października 2012 r. (sygn. akt I OSK 2445/12), w którym sąd odmówił wstrzymania wykonania decyzji Generalnego Inspektora nakazującej wyznaczenie administratora bezpieczeństwa informacji. W uzasadnieniu ww. postanowienia sąd podniósł, że wnioskujący o wstrzymanie wykonania zaskarżonej decyzji nie uprawdopodobnił zaistnienia przesłanek określonych w art. 61 § 3 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2012 r. poz. 270 z późn. zm.) tj. nie wykazał, że w związku z zatrudnieniem osoby na stanowisku administratora bezpieczeństwa informacji czy też utworzenia odrębnych struktur w celu wykonania obowiązku nałożonego zaskarżoną decyzją, zachodzi niebezpieczeństwo wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków. W szczególności, w ocenie Naczelnego Sądu Administracyjnego, nie były przekonywujące podnoszone przez stronę argumenty odnoszące się do powstania istotnych zmian w zakresie zasad bezpieczeństwa organizacyjnego w przedsięwzięciu o charakterze globalnym ani też argumenty dotyczące ewentualnej konieczności ponownego przeprowadzenia ustaleń i konsultacji z organami ds. ochrony danych osobowych.

W 2012 r. zapadł również wyrok w innej sprawie, który nie dotyczył jednak kwestii merytorycznych, lecz formalnych. Na mocy wyroku z dnia 12 kwietnia 2012 r. (sygn. akt II SA/Wa 2826/11) Wojewódzki Sąd Administracyjny w Warszawie uchylił decyzję Generalnego Inspektora Ochrony Danych Osobowych (sygn. DIS/DEC-900/51667/11) i w uzasadnieniu stwierdził, że na podstawie art. 24 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz. U.

---

<sup>246</sup> Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dolożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

z 2000 r. Nr 98, poz. 1071 z późn. zm.), pracownik organu administracji publicznej podlega wyłączeniu od udziału w postępowaniu w sprawie, w której brał udział w wydaniu zaskarżonej decyzji. W ww. sprawie poza sporem było to, że zarówno zaskarżoną decyzję podjętą w wyniku rozpoznania wniosku o ponowne rozpatrzenie sprawy, jak i decyzję ją poprzedzającą, wydał z upoważnienia Generalnego Inspektora Ochrony Danych Osobowych jego Zastępca. W ocenie Sądu, Zastępca Generalnego Inspektora, jako pracownik organu upoważniony do załatwiania spraw w imieniu organu, podlegał wyłączeniu od rozpoznania wniosku o ponowne rozpatrzenie sprawy. Wskazana wada kwalifikowana zaskarżonej decyzji spowodowała, że Sąd nie mógł rozstrzygać sprawy merytorycznie.

W podsumowaniu, na podstawie ustaleń z kontroli przeprowadzonych w 2012 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. Uchybienia te dotyczyły zarówno zastosowanych rozwiązań organizacyjnych, jak i aspektów technicznych.

Ponad 7 % 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 (około 19 % uchybień), jak i instrukcji zarządzania systemem informatycznym, gdzie ponad 13 % opracowanych dokumentów nie zawierało niezbędnych informacji lub też podane informacje nie miały odzwierciedlenia w rzeczywiście zastosowanych środkach organizacyjnych oraz technicznych. W porównaniu z rokiem 2011 odnotowano poprawę w realizacji obowiązków odnoszących się do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych. Około 6 % podmiotów nie prowadziło ewidencji lub ewidencja nie spełniała wymagań określonych w art. 39 ustawy. Zmniejszeniu uległa liczba uchybień dotyczących wyznaczenia administratora bezpieczeństwa informacji, która plasuje się na poziomie 1 %.

W kontrolowanych w 2012 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 (ok. 7 %) oraz braku odnotowywania identyfikatora użytkownika wprowadzającego dane do systemu (poniżej 3 %). 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 5 % systemów). Jednakże porównując dostosowanie systemów informatycznych do wymogów funkcjonalnych określonych w § 7 rozporządzenia, w roku 2012 zauważyć należy poprawę w stosunku do roku 2011. Wszystkie użytkowane systemy informatycznych skontrolowane w 2012 r. umożliwiały 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 sektorach banki i inne instytucje finansowe oraz operatorzy telekomunikacyjni i służba zdrowia, nie stwierdzono w tym zakresie uchybień.

W 2012 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 sytuacji, w których dane były przekazywane poprzez sieć publiczną z wykorzystaniem poczty elektronicznej. Ww. nieprawidłowości dotyczyły 8 % objętych kontrolą systemów informatycznych.

W porównaniu z 2011 r. w analizowanym roku sprawozdawczym poprawie uległo wdrożenie mechanizmów autoryzacji dostępu do danych - we wszystkich objętych kontrolą w 2012 r. systemach informatycznych istniały mechanizmy uwierzytelnienia użytkowników. Nadal jednak - pomimo tego, że skontrolowane systemy informatyczne dysponowały mechanizmem uwierzytelnienia - zdarzały się przypadki niewłaściwego ich stosowania. Stwierdzono również stosowanie nieodpowiednich parametrów haseł do wymaganego poziomu bezpieczeństwa czy też zmianę haseł rzadziej niż raz na 30 dni.

Innym negatywnym zjawiskiem zaobserwowanym w 2012 r. był brak współpracy podmiotu kontrolowanego z inspektorami dokonującymi czynności kontrolnych. Ten brak współpracy przejawiał się w szczególności trudnościami w umówieniu spotkania z osobami reprezentującymi jednostkę kontrolowaną celem okazania imiennych upoważnień i legitymacji służbowych uprawniających do przeprowadzenia kontroli oraz w długim czasie oczekiwania na dokumenty mające bezpośredni związek z przedmiotem kontroli oraz na osoby dysponujące wiedzą o procesie przetwarzania danych osobowych, w celu przyjęcia od nich ustnych wyjaśnień do protokołu. 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 kontrolnej<sup>247</sup>.

W dniach 15-17 kwietnia 2012 r. Komisja Europejska przeprowadziła w Polsce **Misję Ewaluacyjną w zakresie weryfikacji poziomu wdrożenia i utrzymywania dorobku prawnego Schengen**, w tym realizacji zaleceń i wniosków wskazanych w raporcie z I misji oceniającej, przyjętym w dniu 21 kwietnia 2006 r. Głównym celem Misji Ewaluacyjnej było ponadto sprawdzenie obecnego stanu prawnego w zakresie dotyczącym ochrony danych osobowych oraz działań upoważnionych instytucji w zakresie realizacji obowiązku informacyjnego, rozpatrywania skarg obywateli oraz utrzymywania procedur zapewniających na właściwym poziomie ochronę danych osobowych osób, których dane przetwarzane są w systemie informacyjnym Schengen oraz osób zwracających się w tym zakresie o stosowne informacje.

Na uwagę zasługuje tutaj fakt, że od czasu I misji ewaluacyjnej w 2006 roku nastąpiło w powyższym zakresie szereg zmian legislacyjnych. Do najważniejszych należy ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. Nr 165, poz. 1170 z późn. zm.). Ustawa ta określa kompetencje podmiotów w zakresie przetwarzania danych SIS i statuuje uprawnienia kontrolne Generalnego Inspektora Ochrony Danych Osobowych – jako niezależnego organu nadzorczego w rozumieniu art. 114 ust. 1 Konwencji Wykonawczej do Układu z Schengen z dnia 14 czerwca 1985 r. między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej, w sprawie stopniowego znoszenia kontroli na wspólnych granicach. Na mocy tej ustawy Generalny Inspektor Ochrony Danych Osobowych został umocowany do sprawowania kontroli nad tym, czy wykorzystywanie danych (znaczenie tego pojęcia zostało wyjaśnione w art. 2 pkt 18 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym) nie narusza praw osób, których dane te dotyczą. W myśl zaś art. 8 ust. 2 powołanej ustawy, w celu sprawowania powyższej kontroli Generalny Inspektor Ochrony Danych Osobowych został uprawniony do bezpośredniego dostępu do Krajowego Systemu Informatycznego.

Od czasu poprzedniej misji ewaluacyjnej w roku 2006, zmiany nastąpiły również w strukturze organizacyjnej Biura GIODO. Polegały one na połączeniu Departamentu Skarg i Departamentu Prawnego w jeden departament o nazwie Departament Orzecznictwa, Legislacji i Skarg oraz na utworzeniu nowego departamentu - Edukacji Społecznej i Współpracy Międzynarodowej, który przejął zadania i obowiązki realizowane wcześniej przez Departament Prawny w zakresie współpracy międzynarodowej.

---

<sup>247</sup> Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

W programie Misji znalazło się szereg specjalnie przygotowanych przez GIODO, Komendę Główną Policji oraz Ministerstwo Spraw Zagranicznych prezentacji, podczas których omówiono takie zagadnienia jak:

1. status prawny Generalnego Inspektora Ochrony Danych Osobowych, jego zadania, uprawnienia i niezależność w wykonywaniu powierzonych mu obowiązków;
2. struktura organizacyjna Biura GIODO i zakres działań poszczególnych jednostek organizacyjnych;
3. przedsięwzięcia Biura GIODO w zakresie m.in. realizacji kampanii informacyjnych na temat praw i obowiązków osób, których dane dotyczą oraz administratorów, którzy je przetwarzają, w tym zagadnień dotyczących systemów SIS i VIS;
4. sposób zgłaszania i rozpatrywania skarg kierowanych do Biura GIODO w sprawach dotyczących nieprawidłowości w zakresie przetwarzania danych osobowych, w szczególności tych, przetwarzanych na potrzeby systemów SIS i VIS;
5. sposób i zakres prowadzonych przez GIODO kontroli prawidłowości przetwarzania danych osobowych, w tym weryfikacji systemów informatycznych używanych do przetwarzania danych osobowych pod względem wymaganych funkcjonalności oraz zabezpieczeń technicznych i organizacyjnych;
6. organizacja oraz procedury przetwarzania danych osobowych w Biurze SIRENE, które stanowi centrum wymiany danych osobowych przetwarzanych w systemie SIS - w szczególności procedury przyjmowania i załatwiania skarg, wymiany danych z Biurami SIRENE innych krajów, a także stosowane środki i procedury bezpieczeństwa danych przetwarzanych zarówno we własnym systemie obiegu dokumentów, jak i tych, przetwarzanych przy użyciu systemu SIS One4All;
7. organizacja, bezpieczeństwo oraz architektura techniczna Krajowego Systemu Informacyjnego (KSI), którego zadaniem jest utrzymywanie Krajowego Komponentu Systemu Informacyjnego (N.SIS) oraz infrastruktury sieciowej niezbędnej dla połączenia i wymiany informacji z centralnym systemem informacyjnym SIS (C.SIS) zlokalizowanym we Francji;
8. organizacja, bezpieczeństwo oraz procedury i środki zapewniające ochronę danych osobowych przetwarzanych w związku z procesami rozpatrywania wniosków wizowych w systemie VISA-CONSUL, w tym podczas wymiany informacji z systemem SIS.

Generalny Inspektor Ochrony Danych Osobowych wspólnie z MSW był głównym koordynatorem wszystkich spotkań, na których omawiano ww. prezentacje i jednocześnie koordynatorem wymiany informacji, o które zwracali się członkowie Misji Ewaluacyjnej.



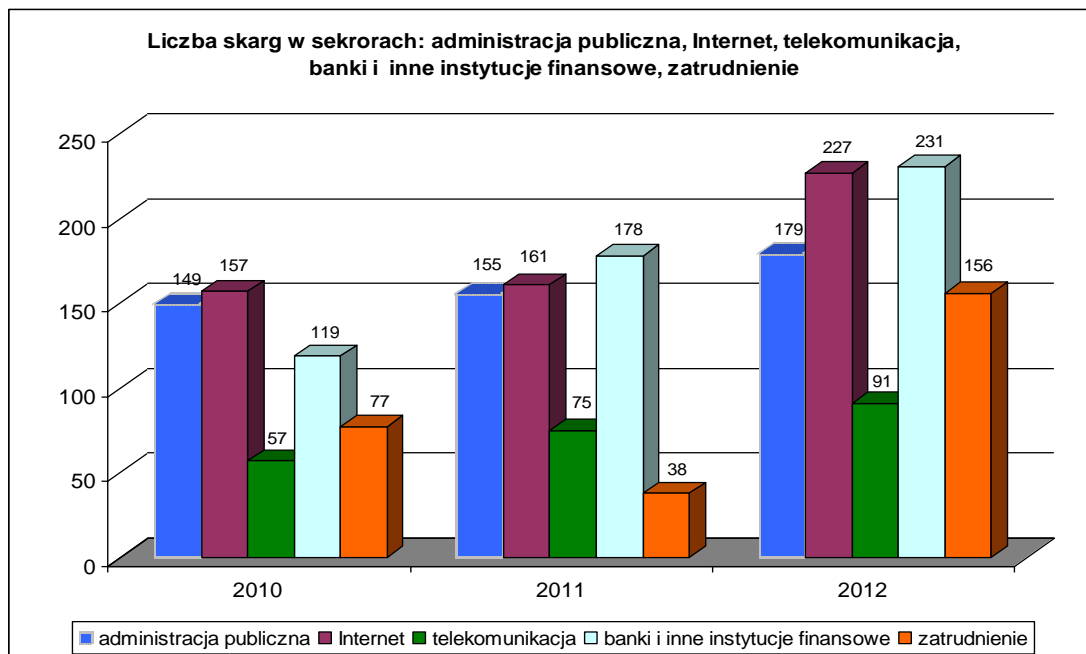
Podkreślenia wymaga, że w ostatecznym raporcie z przeprowadzonej Misji Ewaluacyjnej, Komisja Ewaluacyjna (EvalCom) bardzo wysoko oceniła kompetencje Generalnego Inspektora Ochrony Danych Osobowych podkreślając jego duże osiągnięcia na polu edukacyjnym oraz informacyjnym (specjalnie przygotowane strona eduGIODO oraz zakładka „SCHENGEN” na stronie głównej Biura GIODO dotycząca systemu SIS). Podkreślono tym samym, że zalecenia Misji Ewaluacyjnej z 2006 r. dotyczące GIODO w zakresie rozszerzenia kampanii informacyjnej dotyczącej SIS zostały w pełni wykonane. Komisja Ewaluacyjna wysoko oceniła również narzędzia prawne służące w Polsce ochronie danych osobowych oraz kompetencje Generalnego Inspektora Ochrony Danych Osobowych w sprawowaniu ról nadzorczych i kontrolnych nad ochroną danych osobowych w Polsce.

Niezależnie od powyższego Komisja Ewaluacyjna zasugerowała Generalnemu Inspektorowi Ochrony Danych Osobowych zwiększenie kontroli placówek zagranicznych zajmujących się wydawaniem wiz w celu weryfikacji zabezpieczeń stosowanych w związku z wdrożeniem wizowego systemu Informacyjnego VIS i jego współpracy z systemem SIS. Komisja Ewaluacyjna zwróciła ponadto uwagę na potrzebę usprawnienia przez administratora systemu N.SIS, tj. Komendę Główną Policji, procedur weryfikacji zgodnego z prawem przetwarzania danych w systemie SIS, poprzez systematycznie dokonywanie przeglądu rejestru kierowanych do systemu zapytań i odpowiedzi, w tym przygotowanie narzędzi usprawniających taką weryfikację.

W porównaniu z poprzednimi latami, w 2012 r. można zauważyć systematyczny **wzrost liczby skarg**, które wpłynęły do Biura GIODO. W roku 2008 wpłynęło 986 skarg, w 2009 – 1049, w 2010 – 1114, w 2011 – 1271, zaś w 2012 – 1593. Przyczyn tego wzrostu należy upatrywać przede wszystkim we wzroście świadomości społeczeństwa co do zasad ochrony danych osobowych i jego aktywności w dochodzeniu przysługujących mu praw. Ponadto żądania zawarte w skargach były coraz precyzyjniej formułowane, zaś same podania zawierały mniej braków formalnych, których następstwem byłoby pozostawienie ich bez rozpoznania albo zwrot.

Natomiast porównanie liczby skarg w poszczególnych sektorach na przestrzeni lat 2011-2012 pozwala zauważyć pewne inne interesujące trendy. Pierwszym z nich był znaczący wzrost liczby skarg w sektorze dotyczącym administracji publicznej (rok 2011 - 155, rok 2012 - 179) oraz w sektorze odnoszącym się do działalności banków i innych instytucji finansowych (rok 2011 - 178, rok 2012 - 231). Ten ostatni wskaźnik jest o tyle niepokojący, że w latach 2008-2010 zauważalny był stopniowy spadek liczby skarg na podmioty z tego sektora, sięgający 66 %. O ile w 2008 r. skarg tych było 179, w 2009 – 139, to w 2010 r. wpłynęło ich już zaledwie 119. Natomiast od 2011 r. liczba ta zaczęła wzrastać, by w roku tym osiągnąć 179, zaś w 2012 – 231.

Znaczący wzrost liczby skarg w porównaniu z poprzednim rokiem sprawozdawczym nastąpił także w sektorze działalności internetowej (rok 2011 - 161, rok 2012 - 227), w sektorze telekomunikacyjnym (rok 2011 - 75, rok 2012 - 91) oraz w sektorze zatrudnienia – z 38 skarg w 2011 r. do 156 w 2012 r. W tym ostatnim przypadku oznacza to ponad czterokrotny ich wzrost.



**Wykres 45: Porównanie liczby skarg w sektorach: administracja publiczna, banki i inne instytucje finansowe, Internet, telekomunikacja i zatrudnienie w latach 2010–2012 – trend wzrostowy.**

W pozostałych sektorach liczba skarg prezentuje się na porównywalnym poziomie. W 2011 r. w sektorze dotyczącym działalności sądów, prokuratur, policji i komorników odnotowano 85 skarg, natomiast w 2012 r. - 75, w sektorze marketingu w 2011 r. – 49 skarg, w 2012 r. - 60, w sektorze mieszkalnictwa w 2011 r. – 81 skarg, w 2012 r. - 88 oraz w sektorze ubezpieczeń w 2011 r. – 28 skarg, zaś w 2012 r. - 24.

W podsumowaniu należy zauważyć, że systematycznie 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 bowiem, po interwencji Generalnego Inspektora, podejmowali oni odpowiednie działania zmierzające do zmian kwestionowanych praktyk.

Odnosząc się do faktu corocznego wzrostu liczby wpływających do Biura Generalnego Inspektora skarg związanych z przetwarzaniem danych osobowych, należy wskazać, że przyczyną powyższego był nie tylko fakt naruszania ustawy o ochronie danych osobowych przez administratorów

danych, ale także coraz większa świadomość podmiotów danych w kwestii przysługującej im ochrony z zakresu prawa do prywatności i danych osobowych. Pomimo dużej liczby skarg znacznie zmniejszyła się liczba przypadków, w których organ stwierdził naruszenie ustawy o ochronie danych osobowych. Wynikać to może z konsekwentnej polityki informacyjnej GODO zmierzającej do upowszechnienia wiedzy o prawach i obowiązkach zarówno administratorów danych, jak i osób, których dane dotyczą.

Na konieczności odpowiedniej ochrony danych osobowych wykazują także coraz częściej sami administratorzy danych. 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 zaś do drobnych przedsiębiorców, czy podmiotów pożytku publicznego można zauważyć, że często nie byli oni świadomi faktu, że są administratorami danych osobowych i że spoczywają na nich konkretne obowiązki określone przez przepisy prawa. Odnosząc się zaś do zakresu tematycznego skarg rozpatrywanych w omawianym 2012 roku, zasadniczo nie zauważa się znaczących zmian. W porównaniu z rokiem 2011 problemy pojawiające się we wpływających do Biura Generalnego Inspektora wnioskach uznać należy za tożsame.

W postępowaniach zainicjowanych skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych w 2012 roku z urzędu, wydanych zostało **762 decyzje administracyjne**, z których **70** zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [WSA]. W porównaniu z rokiem 2011, w którym 55 decyzji zostało zaskarżonych, oznacza to wzrost o 15 spraw. Obrazuje to zwiększenie zainteresowania stron postępowań wykorzystaniem przysługujących im narzędzi prawnych w postaci weryfikacji zasadności rozstrzygnięć GODO.

Analizując z kolei działalność **opiniotwórczą** Generalnego Inspektora Ochrony Danych Osobowych w 2012 r., można było dostrzec odnotowaną już w poprzednich okresach sprawozdawczych tendencję do tworzenia przez różne podmioty tzw. megabaz danych osobowych. Wraz z postępującą informatyzacją administracji publicznej, przedmiotem legislacyjnych opinii Generalnego Inspektora Ochrony Danych Osobowych były najczęściej projekty dotyczące unowocześniania istniejących lub tworzenia nowych baz teleinformatycznych. Projektodawcy wychodzili bowiem naprzeciw rozwojowi technologii i tendencji do tworzenia centralnych baz, zasilanych niejednokrotnie danymi z baz o mniejszym zasięgu. Wiele publicznych systemów informacyjnych przechodzi obecnie takie rewolucyjne zmiany, które oprócz niewątpliwych korzyści, niosą ze sobą również liczne zagrożenia, stawiając fundamentalne wyzwania w dziedzinie ochrony prywatności. Dynamiczny rozwój publicznych baz danych powoduje, że nie tylko możliwa, ale znacznie ułatwiona stała się integracja bardzo szczegółowych i wrażliwych informacji o każdym obywatelu. 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 ją możliwości swobodnego dysponowania informacją na swój temat. Dlatego Generalny Inspektor uważnie przygląda się wszelkim przedsięwzięciom w tym zakresie, zwracając baczną uwagę na potrzebę prawidłowego uregulowania zarówno podstaw prawnych funkcjonowania publicznych megabaz danych, jak i prawidłowego rozstrzygania takich kluczowych kwestii jak posiadanie przez określone podmioty statusu administratora danych, administratora systemu informatycznego oraz uprawnień i obowiązków spoczywających na każdej ze stron uczestniczących w procesie przetwarzania danych wynikających z wymogów określonych w obowiązujących przepisach prawa.

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.

Generalny Inspektor Ochrony Danych Osobowych dostrzega i z głębokim przekonaniem popiera ideę informatyzacji działalności podmiotów realizujących zadania publiczne. Jednakże proces ten każdorazowo winien być głęboko osadzony w przepisach prawa o odpowiedniej randze i przygotowany z uwzględnieniem potrzeby adekwatnej oceny i analizy ryzyka oraz dalekosiężnych wymogów ochrony danych osobowych. Stąd przy podejmowaniu działań związanych z budowaniem przez określone podmioty infrastruktury teleinformatycznej i tworzeniu w tym celu odpowiednich podstaw prawnych, należy – na każdym etapie tego procesu – rozważać wpływ konstruowanych rozwiązań na sferę prywatności (*privacy by design*). Koncepcja ta zakłada, iż najważniejsze problemy związane z ochroną prywatności w kontekście funkcjonowania systemów teleinformatycznych należy przewidywać już na etapie procesu legislacyjnego nad aktem prawnym statuującym budowę takich systemów. Powyższe umożliwia bowiem podejmowanie odpowiednich działań ukierunkowanych na zapobieganie występowaniu przedmiotowych problemów, zamiast następczego reagowania na pojawiające się nieprawidłowości. Dlatego Generalny Inspektor Ochrony Danych Osobowych od 2012 r. uczestniczy m.in. w pracach Komitetu Rady Ministrów ds. Cyfryzacji jako organ doradczy, współopiniujący projekty będące przedmiotem prac tegoż Komitetu.

Natomiast odnosząc się do charakterystyki **pytań prawnych** kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2012 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 2012 problematyka opinii prawnych dotyczyła różnorodnych zagadnień. Przez wszystkie lata działalności organu ds. ochrony danych osobowych wciąż aktualne pozostają wątpliwości osób kierujących pytania do GIODO odnośnie legalności przetwarzania danych osobowych w celach windykacyjnych, a tym samym przekazywania tych danych do odrębnych podmiotów. Niezmiennie pojawiają się sygnały o tym, iż firmy windykacyjne przeprowadzając odpowiednie czynności udostępniają dane osobowe dłużnika osobom trzecim. Wśród osób zgłaszających pytania do Generalnego Inspektora Ochrony Danych Osobowych wciąż wiele kontrowersji wzbudzała praktyka sprzedawania wierzytelności za pośrednictwem sieci Internet, a tym samym udostępnianie danych osobowych dłużnika w ofercie takiej sprzedaży. W przypadku zaś przetwarzania danych osobowych przez banki, zgłaszano Generalnemu Inspektorowi wątpliwości odnośnie marketingu stosowanego przez ten podmiot po zakończeniu umowy kredytowej bądź o rachunek bankowy, a także legalności udostępniania i ewentualnego pozyskiwania danych osobowych z Biura Informacji Kredytowej. Niezadowolenie i obawy obywateli wzbudzała też kwestia przetwarzania przez banki danych osobowych klientów, pozyskanych z ich dowodu tożsamości.

W analizowanym okresie powtarzały się pytania odnośnie rejestracji danych osobowych przetwarzanych przez przedsiębiorców prowadzących portale społecznościowe, fora czy też sklepy internetowe. Wiele pytań dotyczyło też sposobu radzenia sobie z naruszeniem prywatności w Internecie, włamywaniem na prywatne konta użytkownika, kradzieżą tożsamości, a także stosowania skutecznych zabezpieczeń danych przetwarzanych za pośrednictwem Internetu.

W grupie pytań kierowanych do Generalnego Inspektora znalazły się także takie, które odnosiły się do pracowników służby więziennej i stosowanej przez nich praktyki imiennego wzywania osób osadzonych w zakładach karnych po odbiór przesyłek i listów na ogólnym forum, a także udostępnianie danych osobowych członków rodzin osadzonych innym współwięźniom. Identyczny problem pojawił się w pytaniach o legalność wyczytywania imion i nazwisk pacjentów w rejestracji, czy też czekających przed gabinetem na wizytę u specjalisty. Ponadto do Generalnego Inspektora Ochrony Danych Osobowych wielokrotnie zwracały się zakłady opieki zdrowotnej z pytaniem, czy mają obowiązek udostępniania danych osobowych wnioskującym o to podmiotom, a także o legalność ich współpracy z firmami zewnętrznymi na podstawie umowy powierzenia.

Wiele pytań kierowanych było również przez podmioty świadczące pomoc społeczną. W szczególności w kwestii udostępniania danych osobowych w ramach kontroli ośrodków pomocy społecznej przez organy samorządowe. Natomiast niepokojące było to, że instytucje świadczące pomoc społeczną miały wątpliwości odnośnie udostępniania osobie, której dane dotyczą, danych zawartych jej w aktach osobowych.

Problematyka opinii prawnych sporządzonych w 2012 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 podmiotów.

W związku z wejściem w życie w dniu 7 marca 2011 r. ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw<sup>248</sup>, organ do spraw ochrony danych osobowych zyskał nowe uprawnienia, w tym możliwość kierowania na podstawie art. 19a ustawy **wystąpień** 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 2012 r. napłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych prowadził do wniosku, że wciąż istnieje wiele regulacji prawnych niejasnych z punktu widzenia ochrony danych osobowych, których interpretacja sprawia trudności zarówno osobom, których dane te dotyczą, jak też i ich administratorom.

Analizując działania GIODO w roku 2012, polegające na udzielaniu odpowiedzi na pytania prawne celem tworzenia wiedzy na temat zasad przetwarzania danych osobowych oraz wykładni przepisów regulujących ten obszar, można stwierdzić, że – podobnie jak w poprzednich okresach sprawozdawczych - istnieje wiele problemów dotyczących przetwarzania danych osobowych nieuregulowanych od strony prawnej, lub też wynikających z ich niedoskonałości bądź błędnej interpretacji. Niepokojące było również to, iż organy administracji publicznej przetwarzały dane osobowe szczególnie chronione, bądź zobowiązywały 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

---

<sup>248</sup> Dz. U. z 2010 r. Nr 229 poz. 1497

należy oceniać praktyki organów pełniących funkcje publiczne, polegające na przetwarzaniu danych osobowych wbrew ich kompetencjom określonym przepisami prawa.

Mającą wciąż zwyżkującą tendencję liczba zapytań nadsyłanych do Generalnego Inspektora Ochrony Danych Osobowych oraz ich zróżnicowana tematyka wskazuje na to, że znajomość norm prawnych w przedmiotowym zakresie jest coraz powszechniejsza, i że są one traktowane przez obywateli jako niezbędny instrument poszanowania jednego z podstawowych praw i wolności. Dziedzina ta podlega ciągłemu i dynamicznemu rozwojowi. Przybywa regulacji prawnych dotyczących przetwarzania danych w różnych sektorach działalności oraz - tym samym - rośnie potrzeba wyjaśniania wzajemnych relacji istniejących norm oraz przydatnej dla ich odpowiedniego stosowania, interpretacji przepisów prawa. Coraz większy stopień skomplikowania tej materii oraz pojawiające się nowe rodzaje zagrożeń prywatności wynikające z dynamicznego rozwoju nowoczesnych technologii (zwłaszcza informatycznych) powodują, że ciągle istnieje potrzeba wyjaśniania licznych wątpliwości oraz podejmowania przez Generalnego Inspektora interwencji w zakresie i w formach przewidzianych przez ustawę o ochronie danych osobowych.

Źródłem wystąpień GODO do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej, albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych, były zarówno luki prawne w dziedzinie ochrony prywatności i respektowania prawa podmiotu danych do ochrony jego danych osobowych, jak i niedokładności w istniejących i nowo tworzonych regulacjach prawnych. Stan taki w następstwie skutkował niejednolitą praktyką administratorów danych, w tym głównie podmiotów publicznych, a tym samym przetwarzaniem danych osobowych przez te same instytucje w różnych zakresach bądź w nieodpowiednich celach.

Zapoznanie się z danymi liczbowymi dotyczącymi działań Generalnego Inspektora Ochrony Danych Osobowych w 2012 r. w zakresie interpretacji przepisów prawa dotyczących ochrony danych osobowych, pozwala uświadomić sobie skalę wciąż wzrastającego społecznego zapotrzebowania na pomoc i interwencję organu ds. ochrony danych osobowych. Przetwarzanie danych osobowych jest bowiem zjawiskiem powszechnym we wszystkich sektorach działalności publicznej, gospodarczej czy społecznej.

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 ustaw<sup>249</sup>. W znowelizowanej ustawie zasadniczy wpływ na zwiększenie poziomu ochrony danych miały 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

---

<sup>249</sup> Dz. U. Nr 229, poz. 1497

egzekucyjnym w administracji<sup>250</sup>, które zdecydowanie zwiększyły skuteczność działań GODO. W ustawie o postępowaniu egzekucyjnym w administracji dodano do obowiązków, które podlegają egzekucji administracyjnej, obowiązki z zakresu ochrony danych osobowych, nakładane w drodze decyzji Generalnego Inspektora Ochrony Danych Osobowych. Powyższe zmiany przyczyniły się znacznie do wzmocnienia pozycji **GODO, który jako organ egzekucyjny w zakresie obowiązków o charakterze niepieniężnym** wynikających z decyzji administracyjnych wydanych w sprawach wykonania przepisów o ochronie danych osobowych mógł, w przypadku niewykonania takiej decyzji administracyjnej przez zobowiązanego, zastosować środek egzekucyjny.

I tak, w związku z praktyką przyjętą przez Generalnego Inspektora Ochrony Danych Osobowych, polegającą na zamieszczaniu we wszystkich decyzjach administracyjnych GODO pouczenia, w treści którego strony były uświadamiane co do skutków niewykonania w terminie nakazów w nich określonych, osiągnięty został cel prewencyjny nowego przepisu. Część spośród decyzji nakazowych GODO była bowiem dobrowolnie wykonywana przez podmioty, do których były one skierowane. Niebagatelną rolę wywarły też zapewne działania edukacyjne i informacyjne Generalnego Inspektora Ochrony Danych Osobowych, który kierował do mediów jasne i czytelne komunikaty, a prelegenci GODO przeprowadzający szkolenia w sposób zrozumiały informowali o zagrożeniu egzekucją administracyjną podmioty niewykonujące decyzji nakazowych GODO. W pozostałych przypadkach wystarczyło w zasadzie dokonanie tzw. czynności sprawdzających, któremu były poddawane zarówno decyzje administracyjne GODO ostateczne, jak i te, którym nadano rygor natychmiastowej wykonalności na podstawie art. 108 § 1 K.p.a. Po upływie terminu wykonania nakazów wymienionych w decyzji GODO, do podmiotu, który nie poinformował o wykonaniu przedmiotowej decyzji, kierowane było wezwanie do złożenia wyjaśnień i przedstawienia dowodów na jej wykonanie. Skuteczna polityka informacyjna i edukacyjna GODO spowodowała, że podmioty niezwłocznie przywracały stan zgodny z prawem i powiadamiały o tym organ do spraw ochrony danych osobowych.

Nowe regulacje umożliwiły skuteczniejsze oddziaływanie organu ds. ochrony danych osobowych na poziom przestrzegania prawa do prywatności i ochrony danych osobowych w Polsce. Dotychczasowe 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. Wpłynęło to korzystnie zarówno na aktualny poziom przestrzegania regulacji dotyczących ochrony danych osobowych (a co za

---

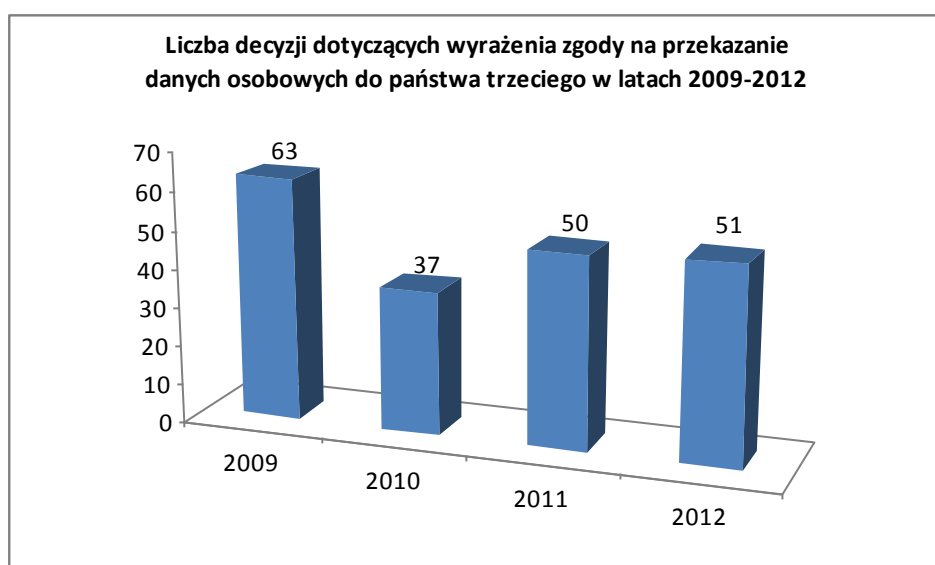
<sup>250</sup> Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.



tym idzie – ogólny stopień ochrony konstytucyjnych praw obywateli), jak i na oddziaływanie prewencyjne w przyszłości.

W 2012 r. do Generalnego Inspektora wpłynęły **93 wnioski o wyrażenie zgody na przekazanie danych osobowych do państw trzecich, tzn. do państw nienależących do Europejskiego Obszaru Gospodarczego (EOG)**. Dla porównania w 2011 r. wpłynęło 65 wniosków o wydanie zgody na przekazanie danych do państw trzecich, czyli o 28 wniosków mniej niż w analizowanym roku sprawozdawczym, natomiast w 2010 – wpłynęło ich 37.

**Ogółem Generalny Inspektor wydał w 2012 r. 51 decyzji administracyjnych dotyczących przekazania danych osobowych do państw trzecich<sup>251</sup>.**



**Wykres 46: Zestawienie porównawcze liczby decyzji dotyczących wyrażenia zgody na przekazanie danych osobowych do państwa trzeciego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2009-2012.**

Spośród wydanych przez GODO decyzji administracyjnych 44 decyzji było pozytywnych, 4 decyzje umarzały postępowanie ze względu na wycofanie wniosków, natomiast dwie decyzje w części były pozytywne, a w części umarzały postępowanie w odniesieniu do odbiorców danych z Konfederacji Szwajcarskiej, co do której Komisja Europejska wydała decyzję o adekwatnym poziomie ochrony danych<sup>252</sup>, wobec czego zgoda Generalnego Inspektora stała się bezprzedmiotowa.

<sup>251</sup> Zgodnie z art. 48 ustawy o ochronie danych osobowych, w przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

<sup>252</sup> Decyzja Komisji z dnia 26 lipca 2000 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie właściwej ochrony danych osobowych w Szwajcarii ((notyfikowana jako dokument nr C(2000) 2304).

Ponadto, w jednej ze spraw Generalny Inspektor częściowo odmówił wyrażenia zgody i częściowo taką zgodę wyraził<sup>253</sup>.

Tak jak w latach ubiegłych administratorzy planujący przekazanie danych do państwa trzeciego najczęściej stosowali standardowe klauzule umowne zatwierdzone przez Komisję Europejską<sup>254</sup>. Należy również odnotować zwiększenie się liczby wniosków dotyczących transferów, do których zastosowano wiążące reguły korporacyjne (WRK).

W sytuacji zastosowania przez administratora danych standardowych klauzul umownych ich charakter prawny wpływa na zakres oceny dokonywanej przez GODO. Należy bowiem pamiętać, że organ ochrony danych osobowych jest obowiązany uznać taki instrument prawny za zapewniający odpowiednie gwarancje praw i wolności osób, których dane dotyczą. W toku postępowania administracyjnego weryfikacji podlega zgodność treści umowy z oficjalną treścią standardowych klauzul umownych. Podkreślenia wymaga, że szczególny status umowy wzorowanej na standardowych klauzulach przysługuje jedynie wtedy, gdy jej postanowienia odwzorowują klauzule zatwierdzone przez Komisję Europejską. Na marginesie należy odnotować błędy w przedkładanych GODO wersjach umów w języku polskim, których można uniknąć stosując klauzule w oficjalnej wersji językowej opublikowanej w Dzienniku Urzędowym UE. W odniesieniu zaś do zakresu oceny wprowadzonych w państwie trzecim zabezpieczeń danych osobowych, a co za tym idzie zakresu żądanych od wnioskodawcy informacji o zastosowanych środkach organizacyjno – technicznych, to jest on uzależniony od rodzaju klauzul. W sytuacji zastosowania obydwu zestawów klauzul znajdujących zastosowanie do przekazania danych pomiędzy administratorami, jest to uzależnione od przewidzianej w klauzulach możliwości wyboru zasad ochrony danych osobowych. Jeżeli strony nie wybiorą w tym zakresie krajowego prawa ochrony danych osobowych właściwego dla eksportera, to oznacza, że nie ma podstaw do badania spełnienia szczegółowych wymogów określonych w rozporządzeniu 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. Jeżeli zaś administrator danych przyjął klauzule mające zastosowanie do przekazania danych na zasadzie ich powierzenia, to w toku postępowania weryfikowana jest zgodność

---

<sup>253</sup> DESiWM/DEC-1155/70235/12 w związku ze złożeniem wniosku o ponowne rozpatrzenie sprawy nie została ona ostatecznie zakończona w 2012 r.

<sup>254</sup> Decyzja Komisji 2001/497/WE z 15.6.2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE, Dz.Urz. WE L Nr 181 z 4.7.2001 r., s. 19; decyzja Komisji 2004/915/WE z 27.12.2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, Dz.Urz. WE L Nr 385 z 29.12.2004 r., s. 74; decyzja Komisji 2010/87/WE z 5.2.2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, Dz.Urz. UE L Nr 39 z 12.2.2010 r., s. 5.

zastosowanych środków z przepisami ww. rozporządzenia. Niemniej nadal możliwy jest pewien margines swobody oceny, czy wdrożone zabezpieczenia zapewniają odpowiedni poziom bezpieczeństwa danych osobowych. W tym miejscu podkreślenia wymaga, że analiza w zakresie technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez podmioty, którym zamierzano przekazywać dane, nadal wskazuje na dosyć częste braki dotyczące funkcjonalności zapewniającej rozliczalność procesów przetwarzania danych w tym głównie warunków wskazanych w § 7 rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Tak jak w latach ubiegłych należy odnotować przypadki przedkładania Generalnemu Inspektorowi do wniosków materiału dowodowego, który nie spełnia wymogów ustawy z dnia 7 października 1999 r. o języku polskim<sup>255</sup>. Kolejnym problemem zidentyfikowanym w praktyce Generalnego Inspektora Ochrony Danych Osobowych jest niedopełnienie przez administratorów danych obowiązków związanych z przetwarzaniem danych na terytorium RP, które mogą mieć znaczenie dla oceny zgodności z prawem przekazywania danych do państw trzecich (np. w odniesieniu do obowiązku zgłoszenia zbiorów do rejestracji).

Biorąc pod uwagę zwiększającą się wśród wnioskodawców popularność WRK, GODO wypracował nowe, kompleksowe podejście do prowadzenia postępowań o wyrażenie zgody na przekazanie danych do państwa trzeciego w sytuacji zastosowania takiego instrumentu prawnego. I tak, biorąc pod uwagę globalny charakter WRK, GODO przyjmuje, iż w założeniu mają one być jednolitym, ogólnoeuropejskim instrumentem prawnym i tym samym powinny odpowiadać wspólnym zasadom określonym przepisami dyrektywy. W konsekwencji, w dosyć szeroko określonych ramach WRK możliwe są przyszłe operacje przekazywania danych, których konkretyzacja może dopiero nastąpić w przyszłości ze względu na określone okoliczności faktyczne z zastrzeżeniem, że administrator danych nie ma tutaj dowolności i jego działania są związane z koniecznością spełnienia pozostałych wymogów ustawy. Powyższe ma też znaczenie dla treści decyzji GODO w takich sprawach oraz sposobu zindywidualizowania poszczególnych importerów danych. Ze względu na to, że WRK mają stanowić generalne ramy zapewniające ochronę danych osobowych w korporacji, a administrator danych ma obowiązek przedstawić aktualną listę importerów danych, to jednak w sentencji decyzji są one indywidualizowane poprzez związanie WRK<sup>256</sup>.

---

<sup>255</sup> Dz. U. 1999 r. Nr 90, poz. 999 z późn. zm.

<sup>256</sup> Por DESiWM-DEC-1272/78196/12, DESiWM/DEC-1273/78191/12, DESiWM/DEC-1275/48200/12; DESiWM/DEC-1276/78213/12; DESiWM/DEC-1281/78303/12; DESiWM/DEC -1282/12/78298/12.

W 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych zgłoszonych zostało do rejestracji **21850 zbiorów**, z czego **14917 zbiorów pochodziło od podmiotów publicznych**, zaś **6663 od podmiotów prywatnych**.

Wśród zgłoszeń do rejestracji pochodzących od **podmiotów publicznych** stosunkowo dużą liczbę stanowiły zbiory danych osobowych zgłaszane do rejestracji przez jednostki oświatowe (przedszkola, szkoły). Jako przykłady można wskazać:

- ✓ zbiory danych prowadzone przez szkoły podstawowe oraz gimnazja w celu realizacji obowiązku polegającego na prowadzeniu ksiąg ewidencji dzieci i młodzieży podlegających obowiązkowi rocznego przygotowania przedszkolnego i obowiązkowi szkolnemu, zamieszkałych w obwodzie szkoły i gimnazjum,
- ✓ zbiory danych osób upoważnionych przez rodziców i opiekunów prawnych do odbioru dzieci odpowiednio ze szkoły lub przedszkola,
- ✓ zbiory danych prowadzone w związku z rekrutacją do szkoły/przedszkola,
- ✓ zbiory danych prowadzone w celu ewidencji korespondencji przychodzącej i wychodzącej,
- ✓ zbiory danych osobowych przetwarzanych w związku z prowadzeniem w jednostkach oświatowych archiwum zakładowego,
- ✓ zbiory danych osobowych przetwarzanych w związku z prowadzonymi postępowaniami o udzielenie zamówienia publicznego.

W omawianym okresie odnotować także należy dużą liczbę zgłoszeń zbiorów danych osobowych prowadzonych na podstawie przepisów ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej (Dz. U. Nr 149, poz. 887 z późn. zm.), które weszły w życie 1 stycznia 2012 r. Przepisy powołanej ustawy regulują m. in. zasady i formy wspierania rodziny przeżywającej trudności w wypełnianiu funkcji opiekuńczo-wychowawczych oraz sprawowania pieczy zastępczej. W świetle przepisów tej ustawy wspieranie rodziny, jako zadanie gminy, to zespół planowanych działań mających na celu przywrócenie rodzinie zdolności do pełnienia tych funkcji. Natomiast system pieczy zastępczej, jako zadanie powiatu, to zespół osób, instytucji i działań mających na celu zapewnienie czasowej opieki i wychowania dzieciom w przypadkach niemożności sprawowania opieki i wychowania przez rodziców. Zbiory danych prowadzone w związku z realizacją tej ustawy zgłaszają do rejestracji przede wszystkim ośrodki pomocy społecznej, które w oparciu o ww. przepisy realizują zadania w gminach w zakresie wspierania rodziny. Natomiast w związku z realizacją zadań powiatu w zakresie pieczy zastępczej zbiory danych osobowych zgłaszają do rejestracji powiatowe centra pomocy rodzinie.

W związku z realizacją **pilotażowego Programu „Aktywny samorząd”** do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były (w szczególności w II

półroczu roku 2012) zbiory danych osobowych dotyczące danych adresatów i beneficjentów tego Programu, tj. osób niepełnosprawnych, które były uprawnione do ubiegania się o dofinansowanie ze środków Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych oraz osób, które takie dofinansowanie otrzymały. Jako podstawę uruchomienia i realizacji Programu „Aktywny samorząd” wskazywany był art. 47 ust. 1 pkt 4 lit a ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2011 r. Nr 127, poz. 721 z późn. zm.). W przepisach rangi ustawowej brak było jednak szczegółowych uregulowań dotyczących tego przedsięwzięcia. Zasady realizacji oraz funkcjonowania Programu regulowały natomiast porozumienia oraz umowy zawierane przez powiaty (realizatorów Programu) z Państwowym Funduszem Rehabilitacji Osób Niepełnosprawnych. Dokumenty te, z punktu widzenia ochrony danych osobowych, zawierały nieprecyzyjne (czy wręcz sprzeczne) postanowienia, co powodowało, iż w związku z realizacją przedmiotowego Programu do rejestracji zgłaszane były zbiory danych osobowych zarówno przez powiatowe centra pomocy rodzinie jak i przez powiaty.

Z przepisów umowy wynikało, iż powiat (realizator Programu) podpisując umowę z Państwowym Funduszem Rehabilitacji Osób Niepełnosprawnych w sprawie realizacji pilotażowego Programu „Aktywny samorząd”, zobowiązany był wskazać jednostkę organizacyjną odpowiedzialną za wykonanie tego zadania (w praktyce były to powiatowe centra pomocy rodzinie). Zgodnie zaś z § 6 wzoru porozumienia, wnioski osób niepełnosprawnych o dofinansowanie ze środków PFRON w ramach Programu, miały być składane, rozpatrywane i realizowane, zaś umowy dofinansowania rozliczane - przez powiatowe centra pomocy rodzinie. Jednocześnie, zgodnie z „Zasadami dotyczącymi wyboru, dofinansowania i rozliczania wniosków o dofinansowanie w ramach pilotażowego Programu *Aktywny samorząd*” – (dział II ust. 4 pkt 4 załącznika nr 1 do wzoru Porozumienia zawieranego w celu skoordynowania działań w ramach programu, będącego załącznikiem nr 2 do uchwały nr 76/2012 Zarządu PFRON z 17 maja 2012 r.), wnioskodawca zobowiązany był złożyć oświadczenie m. in. „*dot. wyrażenia zgody na przetwarzanie danych osobowych przez administratora danych tj. samorząd powiatowy*”.

Biorąc pod uwagę zadania jakie w związku z realizacją pilotażowego Programu „Aktywny samorząd” zostały nałożone na powiatowe centra pomocy rodzinie wydaje się, że właściwym jest stwierdzenie, iż administratorami danych przetwarzanych w związku z realizacją tego Programu były powiatowe centra pomocy rodzinie. Jednakże powołane powyżej przepisy dotyczące zgody na przetwarzanie danych osobowych pozyskiwanej przez powiaty nie pozwalają na takie działanie. Powiatowe centra pomocy rodzinie zgłaszając zbiory danych osobowych do rejestracji kierują się faktycznymi uprawnieniami (faktycznym władztwem) w stosunku do danych podlegających przetwarzaniu. Natomiast powiaty kierują się postanowieniami Porozumień wskazującymi, że są administratorami danych przetwarzanych w związku z realizacją tego Programu.

Sytuacja ta wymagała uporządkowania, dlatego Generalny Inspektor zwrócił się do Prezesa Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych o rozważenie zmiany treści zapisów w powołanych powyżej dokumentach, a zwłaszcza skorygowanie postanowień dotyczących faktycznego władztwa nad danymi osób biorących udział w Programie z treścią załącznika nr 1 do wzoru Porozumienia. Uporządkowanie opisanej sytuacji było niezwykle istotne z punktu widzenia interesów osób biorących udział w Programie. Należy podkreślić, iż legalne przetwarzanie danych szczególnie chronionych wskazanych w art. 27 ust. 1 ustawy o ochronie danych osobowych (w tym danych o stanie zdrowia) jest możliwe po wpisaniu zbioru danych do rejestru zbiorów danych osobowych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych – art. 46 ust. 2 ustawy. Rozbieżności w ocenie, które podmioty były administratorami danych adresatów i beneficjentów Programu skutkowały niemożnością zakończenia postępowań rejestracyjnych prowadzonych w związku ze zgłoszeniami zbiorów danych osobowych tworzonych na potrzeby realizacji pilotażowego Programu „Aktywny samorząd”. W odpowiedzi na ww. pismo Prezes Zarządu Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych zapewnił, iż w planowanej na styczeń 2013 modyfikacji zasad realizacji Programu stosowne zmiany zostaną wprowadzone.

W okresie sprawozdawczym należy odnotować również **zgłoszenia zbiorów danych, w których przetwarzane były wyłącznie dane osób fizycznych prowadzących działalność gospodarczą**. Zgłaszanie takich zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych związane było z uchYLENIEM, z dniem 1 stycznia 2012 r., art. 7a ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej (Dz. U. z 1999 r. Nr 101, poz. 1178 z późn. zm.), który wyłączał dane osobowe zawarte w ewidencji działalności gospodarczej spod przepisów ustawy o ochronie danych osobowych. W wyniku tej zmiany, ochronie przewidzianej w ustawie o ochronie danych osobowych podlegają obecnie dane osób fizycznych bez względu na to, czy osoby te prowadzą działalność gospodarczą, czy też nie. Zauważyć należy jednakże, iż zbiory takie nie były zgłaszane masowo. Jako uzasadnienie takiej sytuacji należy wskazać, że zbiory danych zawierające dane osób fizycznych prowadzących działalność gospodarczą - jeżeli zawierały dane osobowe wykraczające poza zakres zawarty w ewidencji działalności gospodarczej - podlegały obowiązkowi zgłoszenia do rejestracji również w czasie obowiązywania przepisów zawartych w art. 7a ust. 2 ustawy prawo działalności gospodarczej. Jako przykład można wskazać zbiory prowadzone w celu realizacji obowiązków wynikających z ustawy prawo zamówień publicznych, czy zbiory klientów prowadzone w celu realizacji zawartych umów.

Ponadto często miała miejsce sytuacja, że administratorzy danych, którzy przed dniem 1 stycznia 2012 r. przetwarzali dane osób fizycznych prowadzących działalność gospodarczą (w zakresie nie wykraczającym poza zakres zawarty w ewidencji działalności gospodarczej) posiadali również zbiory

danych osób fizycznych, które nie prowadziły działalności gospodarczej i zgłaszali go do rejestracji GIODO. W takim przypadku możliwe były następujące modele zachowania:

- 1) jeżeli dane osób fizycznych prowadzących działalność gospodarczą stanowią odrębny zbiór, administrator zgłasza ten zbiór do rejestracji GIODO,
- 2) jeżeli dane te zostały włączone do zgłoszonego wcześniej zbioru wówczas możliwe są dwa warianty:
  - a) włączenie tych danych powoduje, że w zbiorze zachodzą zmiany (np. zmienia się zakres przetwarzanych danych), co wiąże się z koniecznością dokonania aktualizacji zgłoszonego zbioru,
  - b) po włączeniu tych danych nie zaszły żadne zmiany w zbiorze, w związku z czym nie powstaje obowiązek zgłoszenia zmian w zbiorze.

Jednakże należy zauważyć, że niezależnie od tego, czy na administratorze, który przetwarza dane osób prowadzących działalność gospodarczą, które podlegały wcześniej wyłączeniu spod ustawy o ochronie danych osobowych, ciąży obowiązek rejestracji/aktualizacji zbioru, administrator takich danych zobowiązany jest do uwzględnienia informacji o tych danych w treści dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności w treści polityki bezpieczeństwa w zakresie: 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, a także sposobu przepływu danych pomiędzy poszczególnymi systemami.

W roku sprawozdawczym 2012 do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były również zbiory danych osobowych przetwarzanych w związku z funkcjonowaniem **funduszy inwestycyjnych i emerytalnych**. W szczególności były to zbiory danych dotyczących członków funduszy oraz osób, których dane były przetwarzane w związku z członkostwem innej osoby w funduszu (np. małżonkowie członków funduszu emerytalnego, osoby uprawnione do otrzymania środków zgromadzonych w funduszu po śmierci jego członka), dłużników wierzytelności nabytych przez fundusz sekurytyzacyjny, a także osób, do których kierowane były różnego rodzaju działania marketingowe. W związku z treścią przepisów<sup>257</sup> regulujących działalność funduszy inwestycyjnych i emerytalnych powstała konieczność ustalenia, czy status administratora danych przetwarzanych w zgłoszonym do rejestracji zbiorze przysługiwał funduszowi inwestycyjnemu albo emerytalnemu, czy też towarzystwu funduszy inwestycyjnych albo emerytalnych. W przepisach regulujących funkcjonowanie ww. podmiotów przyjęta została bowiem konstrukcja prawna, zgodnie z którą fundusz inwestycyjny i fundusz emerytalny posiadają osobowość prawną, ale zarządzane

---

<sup>257</sup> Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Dz. U. Nr 146, poz. 1546 z późn. zm.), ustawa z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (Dz. U. z 2010 r. Nr 34, poz. 189 z późn. zm.).

i reprezentowane są odpowiednio przez: towarzystwo funduszy inwestycyjnych albo towarzystwo emerytalne, stanowiące odrębną osobę prawną.

Na tym tle zaistniał m.in. spór pomiędzy Generalnym Inspektorem a jednym z towarzystw emerytalnych, które złożyło zgłoszenia do rejestracji zmian w zbiorach danych stanowiących rejestr członków funduszu emerytalnego oraz w zbiorach danych dotyczących osób, których dane były przetwarzane w związku z zawarciem i wykonywaniem umowy o członkostwo w funduszu (m.in. małżonków członków funduszu emerytalnego, osób uprawnionych do otrzymania środków zgromadzonych w funduszu po śmierci członka funduszu). W przeprowadzonych w związku z ww. zgłoszeniami postępowaniach Generalny Inspektor ustalił, że to fundusz emerytalny jest administratorem ww. danych przetwarzanych w celu realizacji uprawnień i obowiązków funduszu emerytalnego wynikających z ustawy o organizacji i funkcjonowaniu funduszy emerytalnych. Za rozstrzygającą w tym względzie Generalny Inspektor uznał treść przepisów ww. ustawy, które wyznaczają rolę funduszu emerytalnego i towarzystwa emerytalnego w procesie przetwarzania danych osobowych uczestników funduszu oraz innych osób, których dane są przetwarzane w związku z zawarciem i wykonywaniem umowy o członkostwo w funduszu. Wziąć bowiem należy pod uwagę, że jak wskazał Naczelny Sąd Administracyjny, administratorem danych „nie jest (...) każdy dysponent danych osobowych (...). Jest nim ten, kto decyduje o celach i środkach przetwarzania, przy czym zasadnicze znaczenie ma rodzaj i charakter nadanych przez prawo kompetencji (...)”<sup>258</sup>.

Z przepisów rozpatrywanej ustawy wprost wynika, że rejestr członków funduszu emerytalnego prowadzi fundusz emerytalny (art. 89). Również to fundusz emerytalny, a nie towarzystwo, zgodnie z § 4 ust. 3 Rozporządzenia Rady Ministrów z dnia 12 maja 1998 r. w sprawie szczegółowych zasad prowadzenia rejestru członków funduszu emerytalnego, szczegółowego zakresu informacji, które powinny być zawarte w rejestrze, oraz zasad sporządzania i przechowywania kopii danych zawartych w rejestrze na wypadek jego utraty (Dz. U. Nr 63, poz. 402 z późn. zm.), uzyskuje dane wprowadzane do rejestru od członków funduszu i instytucji wykonujących na podstawie odrębnych przepisów zadania w zakresie ubezpieczeń społecznych. Zgodnie z art. 81 ust. 8 i 9 ustawy o organizacji i funkcjonowaniu funduszy emerytalnych, otwarty fundusz otrzymuje dane osobowe członka funduszu, który uzyskał członkostwo w wyniku losowania, a następnie niezwłocznie potwierdza takiemu członkowi na piśmie warunki członkostwa informując go jednocześnie o prawie wskazania osoby lub osób, na których rzecz ma nastąpić po jego śmierci wypłata niewykorzystanych środków oraz o obowiązku złożenia pisemnego oświadczenia o stosunkach majątkowych między nim a jego małżonkiem. W świetle przepisów rozdziału 7 ustawy o organizacji i funkcjonowaniu funduszy emerytalnych nie może też ulegać wątpliwości, że stroną umowy o członkostwo w funduszu

---

<sup>258</sup> Wyrok z dnia 30 stycznia 2002 r. w sprawie o sygn. akt II SA 1098/01.



emerytalnym jest fundusz. W tym kontekście przytoczenia wymaga stanowisko komentatorów, zgodnie z którym „(...) dopuszczalne jest przetwarzanie danych osobowych osoby A przez jej kontrahenta (drugą stronę umowy, osobę B) w taki sposób i w takim zakresie, w jakim jest to niezbędne do wywiązania się z umowy (...). Warunkiem zastosowania omawianego przepisu jest istnienie umowy łączącej tego, czyje dane są przetwarzane, z tym, kto te dane przetwarza”<sup>259</sup>. W świetle powyższego nie sposób uznać, że art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych może stanowić podstawę prawną przetwarzania przez towarzystwo emerytalne danych osobowych członków zarządzanego przez nie funduszu w celu wykonania umowy o członkostwo.

W przypadku, gdy podstawę prawną upoważniającą do prowadzenia zbiorów danych dotyczących osób, których dane są przetwarzane w związku z zawarciem i wykonywaniem umowy o członkostwo w funduszu (np. małżonkowie członków funduszu emerytalnego, osoby uprawnione do otrzymania środków zgromadzonych w funduszu po śmierci jego członka) stanowi art. 23 ust. 1 pkt 2 ustawy, tj. przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów art. 82 ust. 1 i 1a, art. 83 ust. 1 i 2, art. 126, art. 127 czy art. 132 ust. 1 i 3 ustawy o organizacji i funkcjonowaniu funduszy emerytalnych, to te przepisy prawa determinują rolę funduszu emerytalnego jako administratora danych osobowych. Wynika z nich bowiem jednoznacznie, że chodzi o uprawnienia i obowiązki funduszu emerytalnego, a nie zarządzającego nim towarzystwa.

W podsumowaniu wskazać należy za A. Chróścickim, że ustawa o organizacji i funkcjonowaniu funduszy emerytalnych wprowadziła przepisem art. 2 nowy typ osoby prawnej - typu zakładowego lub fundacyjnego<sup>260</sup>. Osoby prawne typu zakładowego różnią się od osób prawnych typu korporacyjnego (np. spółki akcyjne) tym, że dla tych pierwszych podstawowym substratem jest majątek, a nie zespół osób fizycznych. Jednak czynności przetwarzania danych dokonywane były faktycznie przez odpowiednie organy lub osoby fizyczne działające w imieniu administratora danych na podstawie upoważnienia ustawowego lub statutowego lub upoważnienia udzielonego przez administratora danych w przypadku każdej osoby prawnej. W ocenie Generalnego Inspektora Ochrony Danych Osobowych brak jest zatem powodów, dla których należałoby odmówić przymiotu administratora danych w rozumieniu ustawy o ochronie danych osobowych, osobom prawnym typu zakładowego, jak fundusze emerytalne, fundusze inwestycyjne czy fundacje. Towarzystwo emerytalne jest natomiast organem funduszu i jako organ zarządza nim i reprezentuje w stosunkach z osobami trzecimi. Nie ulega zatem wątpliwości, że towarzystwo emerytalne podejmując działania w zakresie zarządzania funduszem i reprezentując go na zewnątrz działa jako organ w imieniu i na rzecz funduszu.

---

<sup>259</sup> J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*. Warszawa 2011, s. 477.

<sup>260</sup> A. Chróścicki, *Ustawa o organizacji i funkcjonowaniu funduszy emerytalnych. Komentarz*. Wyd. Oficyna, Warszawa 2010.

Niniejsza sprawa stała się przedmiotem postępowania przed Wojewódzkim Sądem Administracyjnym, który podzielił stanowisko Generalnego Inspektora oddalając skargi Towarzystwa Emerytalnego. Podkreślenia wymaga także, że towarzystwa funduszy inwestycyjnych i towarzystwa emerytalne są administratorami danych osobowych m.in. w przypadku, jeśli działając we własnym imieniu i na własny rachunek przetwarzają dane osobowe (również dotyczące członków zarządzanych przez siebie funduszy) dla własnych celów marketingowych, gdy osoba, której dane dotyczą wyrazi na to zgodę. Tego typu zbiory danych służące celom marketingowym wpisane są do prowadzonego przez Generalnego Inspektora rejestru.

## **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 prawa do prywatności i ochrony danych osobowych. Poszerzają się zwłaszcza obszary wymiany informacji i zbierania danych osobowych oraz powstaje coraz więcej baz gromadzących dane osobowe pochodzące z różnych źródeł. Nie ulega wątpliwości, że państwo powinno posiadać zasób informacyjny dotyczący obywateli, a także innych podmiotów i dlatego buduje scentralizowane systemy, które mają mu tę wiedzę zapewnić. W latach 2011-2012 stworzono podstawy prawne dla kilku istotnych z punktu widzenia państwa systemów informacyjnych, które przyjęły postać megabazy - w ochronie zdrowia, oświacie oraz w sektorze nauki i szkolnictwa wyższego. Wprowadzono też nowe rozwiązania dotyczące elektronicznych ksiąg wieczystych. I choć w przypadku tych systemów

zakończył się już proces prac legislacyjnych na poziomie Sejmu, to przed organem ds. ochrony danych osobowych stało zadanie monitorowania ich pracy.

W 2012 r. kontynuowane były prace nad zintegrowanym systemem informacji o nieruchomościach, a także projektem pl.ID (elektroniczny dowód osobisty), obejmującym m.in. przebudowę rejestru PESEL oraz budowę Centralnego Rejestru Aktów Stanu Cywilnego (CRASC) i Rejestru Dowodów Osobistych (RDO). Wszystkie te przedsięwzięcia łączy interoperacyjność, czyli możliwość wspólnego korzystania lub wymiany danych pomiędzy systemami. Dlatego wciąż otwartym pozostaje pytanie o to, kto zarządza uprawnieniami dającymi dostęp do tych systemów. W ramach projektu pl.ID, dzięki bezpłatnemu podpisowi elektronicznemu zapisanemu w dowodzie, możliwe będzie korzystanie za pomocą Internetu z usług oferowanych przez urzędy. Z drugiej jednak strony mają powstać rozwiązania techniczne, które umożliwią urzędnikowi elektroniczny dostęp do różnych rejestrów publicznych prowadzonych przez inne urzędy. Stąd ogromnym wyzwaniem dla GODO 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 obywateli przed profilowaniem lub kradzieżą tożsamości.

W Polsce mamy wiele powszechnie dostępnych rejestrów dla obywateli, np. Rejestr Ksiąg Wieczystych czy Krajowy Rejestr Sądowy, jak i rejestry dostępne wyłącznie dla urzędników, np. Krajowy Rejestr Karny zawierający dane wrażliwe, aby ci mogli wydobywać z nich konkretne informacje celem przekazania obywatelowi lub upoważnionej instytucji. W tym miejscu należy podkreślić, że wiele z tych tak kosztownie chronionych danych podstawowych jest łatwo dostępnych poza tymi systemami. Nierzadkie są więc opinie, że ochrona danych osobowych powinna skupiać się przede wszystkim na danych wrażliwych, wymagających szczególnej ochrony. Bez umniejszania potrzeby tworzenia scentralizowanych rejestrów danych, wskazuje się też na możliwość tworzenia mniejszych, lokalnych baz, z których można byłoby pozyskiwać dane potrzebne do realizacji konkretnych zadań publicznych, minimalizując w ten sposób pokusę utrzymywania megabaz. Dlatego konieczny jest przegląd rejestru danych pod kątem eliminacji nadmiaru informacji, powściągliwość w generowaniu nowych baz, a także zapewnienie możliwości wymiany danych, które powinny być dobrze strzeżone, przetwarzane zgodnie z prawem i właściwie usuwane. Konieczne są także bariery przed nieuzasadnionym profilowaniem, aby jednostka nie miała poczucia, że informacje o niej gromadzone mogłyby zostać wykorzystane przeciwko niej bez odpowiedniej kontroli prawnej.

Należy też zastanowić się nad działaniami zapewniającymi w praktyce większą skuteczność przepisów karnych dotyczących ochrony danych osobowych tak, aby podmioty państwowe czy gospodarcze, które łamią zasady ochrony prywatności i danych osobowych, nie miały poczucia bezkarności. W tym miejscu należy podkreślić, że nie ma i nie będzie stuprocentowego zabezpieczenia

danych. Ich najsłabszym ogniwem jest człowiek. O ile w przypadku bezprawnego udostępnienia danych, np. z rejestru karnego, do którego nie da się przeniknąć bez pozostawienia elektronicznego śladu, o tyle w odniesieniu do ogólnodostępnych rejestrów można bez problemu różne dane pozyskać.

W 2012 r. Generalny Inspektor Ochrony Danych Osobowych kontynuował prace merytoryczne w takich obszarach **jak monitoring i sieci inteligentne**. Zagadnienie monitoringu wizyjnego sygnalizowane było przez organ również w poprzednich okresach sprawozdawczych, poprzez wskazanie na brak kompleksowej regulacji prawnej w formie ustawy. W odniesieniu do tego zagadnienia istnieją jedynie uregulowania cząstkowe, m.in. o wykorzystaniu monitoringu w więzieniach czy podczas imprez masowych. Generalny Inspektor Ochrony Danych Osobowych niejednokrotnie zwracał uwagę na konieczność regulacji monitoringu wizyjnego w placówkach oświatowych, w szpitalach, czy w zasobach mieszkaniowych oraz tam, gdzie monitoring rozwija się bardzo dynamicznie – w sektorze prywatnym. Dlatego przygotował materiał prezentujący wkład GIODO do oczekiwanej ustawy o monitoringu wizyjnym, który został zaprezentowany podczas Międzynarodowej Konferencji „Miasto monitorowane, personel, aspekty prawne i technika systemów CCTV” współorganizowanej przez Krajową Radę Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej, która odbyła się w dniach 17-18 maja 2012 r. w Częstochowie. W opracowaniu tym 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.

Tematyka monitoringu wizyjnego oraz jego społeczny odbiór prezentowana była również na konferencji zorganizowanej przez Rzecznika Praw Obywatelskich i Generalnego Inspektora Ochrony Danych Osobowych pod tytułem „Kto na nas patrzy? Obywatel pod obserwacją kamer” w dniu 11 października 2012 r. w Warszawie. Podczas tego spotkania Generalny Inspektor wskazał na niedostatki w prawnej regulacji korzystania z monitoringu przez organy ścigania (brak określenia dozwolonych parametrów i funkcji instalowanych w przestrzeni publicznej urzędzeń, brak procedury oceny zasadności instalacji kamer w określonym miejscu, zasad przetwarzania nagrań pochodzących z monitoringu, wymagań wobec operatorów kamer, czy obowiązków informacyjnych podmiotu prowadzącego monitoring). GIODO uznał za konieczne zapewnienie jawności i transparentności funkcjonowania monitoringu i zaangażowanie wspólnot lokalnych w ocenę potrzeby jego instalacji.

Istotą problemu związanego z monitoringiem wizyjnym upatrywać należy z zagadnieniem definicji danych osobowych. Danymi osobowymi nie są bowiem informacje, których nie można

przypisać do konkretnej osoby, lub gdy ustalenie jej tożsamości wymagałoby nadmiernych nakładów czasu, kosztów i działań (art. 6 ust. 3 ustawy o ochronie danych osobowych). Jeśli zatem wizerunek utrwalony na taśmach wideo np. z monitoringu osiedlowego, można połączyć z danymi z rejestru członków spółdzielni, to w takiej sytuacji zastosowanie znajdują przepisy ustawy o ochronie danych osobowych. To zatem, czy zapis wideo połączony jest z innymi danymi osobowymi i jakie jest kryterium dostępu do tych danych, zależy od organizacji wideofilmowania. W takim razie zachodzi konieczność – wobec wspomnianego braku uregulowań prawnych monitoringu – każdorazowej oceny sytuacji występującej u danego administratora w odniesieniu do definicji danych osobowych sformułowanej ww. art. 6. Legalność z punktu widzenia przepisów o ochronie danych osobowych można oceniać dopiero wtedy, gdy okaże się, że zapis na taśmach wideo można traktować jak dane osobowe w rozumieniu ustawy. Wówczas administrator musi wykazać się spełnieniem jednej z przesłanek określonych w art. 23 ust. 1 ustawy. Dotychczas spółdzielnie mieszkaniowe gromadzące w ten sposób dane osobowe powoływały się na pkt 5 tego przepisu, zezwalający na wykorzystywanie danych, gdy służy to realizacji usprawiedliwionego celu administratora, wskazując na potrzebę zapewnienia bezpieczeństwa budynku i mieszkańców lub ochronę majątku spółdzielni.

Innym ważnym tematem było zagadnienie inteligentnego pomiaru i związane z nim zagrożenia prywatności w związku z toczącym się procesem wdrażania inteligentnych sieci w Polsce i pojawieniem się nowych podmiotów w architekturze inteligentnego rynku energii, jak Operator Informacji Pomiarowej (OIP) czy agregatorzy. Rozwój komunikacji elektronicznej w ramach *smart grid* stał się poważnym wyzwaniem nie tylko dla energetyki i sektora telekomunikacyjnego, ale także dla organu ochrony danych osobowych, w kontekście zapewnienia, z jednej strony - bezpieczeństwa energetycznego kraju i ochrony prywatności z drugiej. W odniesieniu do koncepcji budowy inteligentnych sieci energetycznych, Generalny Inspektor Ochrony Danych Osobowych szczególną uwagę zwraca na wynikające z przepisów o ochronie danych osobowych zasady, takie jak ograniczenie zakresu przetwarzania danych do minimum niezbędnego z punktu widzenia celu, który ma być osiągnięty oraz konieczności zabezpieczenia danych przed ich ujawnieniem osobom nieuprawnionym. Uwzględniając fakt, że przy wdrażaniu technologii inteligentnego pomiaru oraz inteligentnych sieci wykorzystuje się najnowsze rozwiązania z zakresu informatyki i telekomunikacji, wskazywał na potrzebę uwzględniania mechanizmów i procedur służących ochronie danych osobowych już na etapie projektowania i tworzenia systemu. Występujące w tym zakresie zagrożenia oraz rekomendacje dotyczące stosowania inteligentnych liczników zebrane zostały w opracowaniu zatytułowanym „Inteligentne liczniki – czy są niezbędne, w czym pomagają i jakie wątpliwości budzą ich instalacje”. Tezy zawarte w tym opracowaniu zaprezentowane zostały na konferencji „Inteligentne sieci - rynek, konsument i zasada zrównoważonego rozwoju”, zorganizowanej przez Urząd Regulacji Energetyki w dniu 18 września 2012 r. w Warszawie oraz na konferencji „II Smart Communications &

Technology Forum”, zorganizowanej przez Center for Business Education w dniu 27 września 2012 r. w Gdańsku.

Nowoczesne technologie – zwłaszcza informatyczne - w erze globalizacji są postrzegane jako kluczowe czynniki wpływające na konkurencyjność, rozwój gospodarczy, edukację, zatrudnienie i integrację społeczną. Wiele młodych osób dostrzega głównie pozytywne strony postępu technologicznego, zbyt pochopnie ignorując tę drugą. Nie sposób zaprzeczyć np. wygodzie korzystania z kart bankomatowych, ale z drugiej strony nietrudno zauważyć, że dzięki kartom banki uzyskują informację o naszych wydatkach i preferencjach z tym związanych, a także mogą nas bez problemu zlokalizować poprzez zainstalowane w nich czipy. Przykłady można by mnożyć, ale chyba najbardziej kontrowersyjnym wydaje się być koordynowany w Polsce unijny projekt pod nazwą **INDECT**,<sup>261</sup> pod którym kryje się system informacyjny wspierający obserwację, wyszukiwanie i wykrywanie niebezpiecznych zdarzeń i przedmiotów dla celów bezpieczeństwa obywateli w środowisku miejskim. Dzięki automatu dotychczas stosowany stały monitoring wszystkich i wszystkiego ma być zastąpiony monitoringiem zagrożeń, poprzez wykorzystanie innowacyjnych algorytmów wspomaganie decyzji człowieka w zwalczaniu terroryzmu i innych działań przestępczych, wykrywaniu niebezpiecznych sytuacji i niebezpiecznych przedmiotów w przestrzeni publicznej. Komputerowej analizie mają być poddawane obrazy z inteligentnych kamer monitorujących przestrzeń publiczną, wyposażonych w funkcję scalającą obraz i dźwięk, dane z portali społecznościowych, publikacji na blogach czy forach internetowych oraz dane z wyszukiwarek. System ma także wykorzystywać identyfikację twarzy konkretnych osób, danych biometrycznych oraz informacje o lokalizacji telefonów komórkowych.

Gromadzeniu przez służby specjalne jak najwięcej informacji ingerujących w życie prywatne obywateli odbywa się pod hasłem zapewnienia bezpieczeństwa. Obowiązujące w Polsce przepisy prawa nie dają pełnej gwarancji ochrony prywatności obywateli, zaś Komisja Europejska wskazała Polskę, jako na kraj, w którym służby najczęściej korzystają z możliwości pobierania danych od operatorów sieci komórkowych, i to nie tylko policję i służby specjalne. A jeśli do tego dodamy jeszcze usługę Google Street View, to skala zjawiska inwigilacji obywateli przez różne podmioty może okazać się znacząca.

---

<sup>261</sup> Projekt INDECT - współfinansowany ze środków Unii Europejskiej – realizowany jest przez uniwersytety i ośrodki badawcze w 12 państwach członkowskich UE. Propozycja projektu INDECT została zgłoszona przez grupę 17 europejskich partnerów pod przewodnictwem Akademii Górniczo-Hutniczej w Krakowie. AGH zaprosiła do współpracy nad tym projektem Politechnikę Gdańską i Politechnikę Poznańską. Na potrzeby realizacji całego przedsięwzięcia utworzone zostało konsorcjum, w skład którego wchodzi wiele instytucji, jak Uniwersytet w Madrycie, w Yorku, w Wuppertalu i w Grenoble, Politechnika w Sofii, w Ostrawie i w Koszycach, Uniwersytet Nauk Stosowanych z Wiednia, a także spółki komercyjne i przyszli odbiorcy. INDECT jest naukowym projektem badawczym, nie zaś wdrożeniowym. Przewidywany czas trwania projektu obejmuje lata 2009-2013.

Ponadto w związku z ustaleniami z kontroli GIODO przeprowadzonych u podmiotów świadczących **usługi w sieci** okazało się m.in., że np. niektóre sklepy internetowe wprowadzają procedury związane z transmisją instrumentów uwierzytelniających w trakcie zakładanie kont w serwisach internetowych, co niesie ze sobą ryzyko upublicznienia danych osobowych. Ww. podmioty przesyłają instrumenty uwierzytelniające, umożliwiające dostęp do danych osobowych w formie jawnej za pośrednictwem wiadomości e-mail, która może zostać przechwycona w każdym punkcie tego "łańcucha dostaw" przez dowolnego użytkownika z dostępem do tych serwerów, np. administratora serwera po stronie nadawcy, odbiorcy lub dostawcy Internetu. Należy także wziąć pod uwagę możliwość włamania się przez cyberprzestępców na dowolny serwer z dostępem do Internetu w celu kradzieży informacji.

Dlatego GIODO w ramach różnych akcji informacyjno - edukacyjnych niezmiennie apeluje do to, aby czytać informacje zawarte w polityce prywatności i regulamin podmiotu świadczącego usługi w sieci, zanim powierzemy mu swoje dane. Każdy taki podmiot powinien w nich podać dane właściciela serwisu, jego siedzibę i informację o tym, jak zamierza przetwarzać dane osobowe. Jeśli zaś używamy poczty elektronicznej, której dostawca składa dane w chmurach (w modelu *cloud computing*), to możemy tylko stwierdzić, na którym z serwerów się znajdują, z którego korzysta obsługująca nas firma. I chociaż wielu przedsiębiorców oferujących usługi *cloud computingu* zapewnia swoich klientów, że ich dane będą przetwarzane wyłącznie w centrach zlokalizowanych na terenie UE lub EOG, to pojawić się może problem danych będących tajemnicami prawnie chronionymi, których przekazywanie do innego kraju może być przestępstwem. Dlatego organy ochrony danych osobowych proponują, by problem ten rozwiązać przyjmując tzw. wiążące reguły korporacyjne. Korporacja, która dostarcza chmurę, przyjmowałaby określony zestaw reguł, tworząc w ten sposób „wirtualne państwo” zapewniające ochronę powierzonych jej danych osobowych.

Pamiętać także należy, że świadomie udostępnione dane osobowe mogą być wykorzystane przez podmiot przetwarzający te dane również w innym niż w pierwotnie wskazanym celu – na przykład do **profilowania**. Niepokój organu do spraw ochrony danych osobowych budzi coraz powszechniejsze zjawisko zbierania danych osobowych ze źródeł ogólnie dostępnych (np. z Internetu), uzupełnianie ich z innych legalnych źródeł, a następnie dokonywania zestawień porównawczych z danymi statystycznymi charakterystycznymi dla wybranych cech konkretnego podmiotu danych, np. w kwestii długości życia, ze względu na wiek, płeć, wykonywany zawód czy przebyta chorobę. Wnioskowanie to jest zaledwie prawdopodobne, niemniej chętnie stosowane w bankach czy firmach ubezpieczeniowych w celu oszacowania ryzyka ubezpieczyciela i dopasowania oferty do klienta. Na tym przykładzie widać wyraźnie, że profilowanie umożliwia „tworzenie nowych danych osobowych” – innych niż te, które osoba sama podała lub których znajomości przez administratora mogła się spodziewać. Przypisanie

danej osobie profilu może prowadzić do nieusprawiedliwionego pozbawienia jej dostępu do pewnych dóbr i usług, i tym samym do naruszenia zasady niedyskryminacji.

Profilowanie co do zasady nie jest działaniem nielegalnym. Niemniej GIODO zwraca uwagę, że każdy, kto dokonuje profilowania, ma obowiązek poinformowania o tym podmiotu danych. Wypełnienie obowiązku informacyjnego wobec osoby profilowanej nie jest w Polsce wykonywany, tymczasem obowiązek ten podkreśla rekomendacja Rady Europy z dnia 23 listopada 2010 r. w sprawie tworzenia profili i ochrony danych<sup>262</sup>, określającą minimalne standardy ochrony prywatności.

Przed organem do spraw ochrony danych osobowych na nadchodzący 2013 rok stoi też inne ważne zadanie, związane z postulowanymi w prawie UE **prawie do zapomnienia**. Dzięki wdrożeniu tej regulacji zyskalibyśmy prawo do skutecznego wycofania z sieci informacji na nasz temat oraz domagania się, aby nie była ona nadal przetwarzana w dużych systemach informatycznych. Zadanie to jest trudne do realizacji nie tylko w praktyce, ale także do ujęcia w przepisach prawa.

Należy również zasygnalizować, że dużą rozwałą powinny kierować się osoby instalujące **aplikacje mobilne na urządzeniach przenośnych**. Poza korzyściami związanymi z wykorzystywaniem ww. aplikacji, one również niosą ze sobą potencjalne zagrożenia dla prywatności ich użytkowników. Poprzez możliwość odczytania wszystkich danych kontaktowych zapisanych w urządzeniu. Kolejną nowością, która pojawiła się w Polsce jest możliwość dokonywania **płatności zbliżeniowych**, które mogą być realizowane z poziomu smartfonów wyposażonych w technologię NFC. Poza korzyściami związanymi z możliwością dokonywania zakupów produktów oraz usług płacąc zbliżeniowo za pomocą karty płatniczej w telefonie mogą pojawić się również zagrożenia związane z możliwością odczytania numeru karty przez nieuprawnione osoby.

W analizowanym 2012 r. – podobnie jak w poprzednim roku sprawozdawczym – Generalny Inspektor Ochrony Danych Osobowych zajmował się sprawą prawnego uregulowania przez właściwe organy, problemu **usuwania informacji publicznej zamieszczonej w Internecie**, wobec braku określenia okresu dostępności danych osobowych na stronach internetowych urzędów lub w Biuletynie Informacji Publicznej, w szczególności braku wskazania końcowego terminu ich publikacji.

W odpowiedzi na wystąpienie GIODO resort administracji i cyfryzacji przyznał, że przepisy prawa dotyczące udostępniania informacji publicznej w Internecie powinny być doprecyzowane co do tego, w jakich przypadkach i jak długo na stronach internetowych mogą być dostępne dane osobowe objęte informacją publiczną. Niezbędnych zmian będzie można dokonać przy okazji nowelizacji ustawy o dostępie do informacji publicznej. W opinii GIODO, problem ten nabiera szczególnego znaczenia w obliczu wprowadzenia do polskiego porządku prawnego regulacji dotyczących ponownego wykorzystywania informacji publicznej.

---

<sup>262</sup> zob. [http://www.giodo.gov.pl/230/id\\_art/3920/j/pl/](http://www.giodo.gov.pl/230/id_art/3920/j/pl/)



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, ponieważ właśnie do tej sfery przenieśliśmy w dużej mierze naszą obecność i komunikację. Zbieranie, agregacja i analiza danych potencjalnych klientów stanowi często ważną część działalności gospodarczej przedsiębiorstw. Dane osobowe, kwestie ich zbierania i analizy są obwarowane wieloma wymogami formalnymi, które w przypadku małych średnich przedsiębiorstw (MŚP) nieposiadających solidnego zaplecza prawnego oraz wystarczającej liczebności, bywają znaczącymi przeszkodami w rozwoju młodej przedsiębiorczości, która napędza rynek usług w sieci. Dlatego GODO musi obrać właściwy kierunek swych działań, aby pojawiła się jakakolwiek szansa na odbiurokratyzowanie tego obszaru. System edukacji powinien wesprzeć wysiłki zmierzające do szybkiej i powszechnej cyfryzacji kraju. Brak zaufania do technologii informatycznych może bowiem stać się poważną barierą dla rozwoju gospodarczego i blokować rozwój europejskiego jednolitego rynku. Stąd przed organem ds. ochrony danych stoi bardzo ważne zadanie związane 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. Dlatego ochrona danych osobowych odgrywa tak ważną, wręcz kluczową rolę w Europejskiej Agendzie Cyfrowej<sup>263</sup> i strategii „Europa 2020”<sup>264</sup>.

Obszar działań Generalnego Inspektora Ochrony Danych Osobowych jest bardzo szeroki i wymaga kompetencji organu w wielu różnych dziedzinach prawa, nauki czy gospodarki w związku z planowanymi zmianami w obecnie obowiązujących regulacjach dotyczących przetwarzania danych osobowych. W ramach prac nad tzw. **pakiem deregulacyjnym**, które toczyły się w resorcie gospodarki, Generalny Inspektor Ochrony Danych Osobowych podjął działania nad wprowadzeniem przepisów ułatwiających pracę podmiotom przetwarzającym dane. Obecnie wszystkie podmioty, które przetwarzają dane w zbiorach danych osobowych, muszą zgłaszać ten fakt do GODO. Planowana **nowelizacja** zdejmie z przedsiębiorców ten obowiązek, ale tylko pod warunkiem, że zatrudniają administratora bezpieczeństwa informacji (ABI) i zgłoszą ten fakt Generalnemu Inspektorowi Ochrony Danych Osobowych. Obowiązek zgłoszenia zbioru danych osobowych do rejestracji GODO zostanie utrzymany w przypadku, gdy zbiór ten zawierać będzie dane wrażliwe, na co potrzebne jest zezwolenie organu ds. ochrony danych na ich przetwarzanie. Kolejną propozycją będzie rezygnacja z kontroli

---

<sup>263</sup> COM(2010) 245 wersja ostateczna.

<sup>264</sup> COM(2010) 2020 wersja ostateczna.

wykorzystywania przez firmę zgromadzonych danych. Obecnie czynności kontrolne przeprowadzane są przez inspektorów GIODO, zaś w planowanej nowelizacji ustawy przewidywana jest możliwość dokonywania kontroli przez administratorów bezpieczeństwa informacji. Przedsiębiorcy sami będą mogli zdecydować, czy powołać u siebie takiego administratora. Zdaniem organu ds. ochrony danych osobowych w planowanej noweli powinien istnieć przepis prawa, zgodnie z którym administrator danych będzie mógł powołać administratora bezpieczeństwa informacji. Jeżeli się na to zdecyduje, to będzie mógł skorzystać z udogodnienia, które planuje wprowadzić nowelizacja ustawy.

Wśród nowych technologii uwagę Generalnego Inspektora zwróciła także coraz powszechniejsza usługa *cloud computingu*. Na jej wdrażanie decyduje się coraz więcej podmiotów skuszonych wizją łatwiejszego dostępu do narzędzi IT oraz redukcją kosztów. Otoczenie technologiczne zmienia się bardzo szybko. Coraz powszechniejszym zjawiskiem stało się przetwarzanie danych osobowych w chmurze obliczeniowej, co wymusza na środowisku zajmującym się ochroną danych konieczność precyzyjnego określenia zadań na nadchodzące lata w tym obszarze. Konieczne jest przede wszystkim wzmocnienie działań informacyjnych organu do spraw ochrony danych osobowych w kwestii uświadomienia odpowiedzialności klienta usług w chmurze jako administratora danych. Dlatego zaleca się, aby klient usługi chmurowej wybierał takiego dostawcę usług *cloud computingu*, który zagwarantuje zgodność z prawodawstwem UE z zakresu ochrony danych, a zawarta z nim umowa zawierała wystarczające gwarancje co do środków technicznych i organizacyjnych. Istotne jest również zalecenie, aby klient zweryfikował, czy dostawca usług w chmurze może zagwarantować zgodność z prawem wszelkich operacji międzynarodowego przekazywania danych.

Jak już o tym była mowa w innej części Sprawozdania, w styczniu 2012 r. Komisja Europejska zaproponowała **pakiet zmian prawa Unii Europejskiej**. Jedną z propozycji był projekt ogólnego rozporządzenia o ochronie danych osobowych, który wprowadził wiele nowych rozwiązań w kwestii zapewnienia skutecznej ochrony danych osobowych obywateli państw UE. Wśród nich najważniejsze było m.in. zagwarantowanie ujednoliconych przepisów, które będą obowiązywać w całej Unii, łatwiejszego dostępu do informacji na temat przetwarzania dotyczących nas danych osobowych oraz o przypadkach naruszeń ich bezpieczeństwa. Ponadto unijne przepisy byłyby stosowane także wobec przedsiębiorstw spoza UE, które oferują towary i usługi na terytorium Wspólnoty (np. za pośrednictwem Internetu), zwiększona będzie odpowiedzialność podmiotów przetwarzających dane osobowe oraz zapewniona możliwość złożenia skargi w swoim kraju, nawet w przypadku, gdy dane osobowe przetwarzane były na terytorium innego państwa. Wysoki poziom ochrony danych osobowych przyniesie również korzyści przedsiębiorcom. Jeśli obywatele mają zaufanie do tego, co dzieje się z dotyczącymi ich danymi osobowymi, wówczas chętniej korzystają z usług, które wymagają podania takich danych. Dzięki temu rozwija się rynek online i gospodarka cyfrowa. Reforma usprawni

też funkcjonowanie jednolitego unijnego rynku, co powinno przełożyć się na wzrost gospodarczy i powstanie nowych miejsc pracy. Tam, gdzie nie pociągałoby to zagrożenia dla praw obywateli, usunięta byłaby także zbędna biurokracja przy przekazywaniu danych osobowych do państw trzecich, przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa. Ponadto zmniejszeniu uległaby liczba formalności administracyjnych (np. obowiązek zgłoszenia zbioru do organu nadzorującego) przy jednoczesnym zwiększeniu roli i odpowiedzialności samych przedsiębiorców, którzy odpowiedzialiby przed jednym organem ochrony danych osobowych niezależnie od tego, w ilu państwach UE prowadzą działalność. Wobec wszystkich przedsiębiorców stosowane byłoby to samo prawo o ochronie danych osobowych, nie zaś różne regulacje krajowe.

W tym miejscu należy podkreślić, że nadal trwają prace nad niektórymi elementami unijnej reformy ochrony danych osobowych. Zalicza się do nich zagadnienie zgody na przetwarzanie danych (art. 4 pkt 8 projektu rozporządzenia), profilowania (art. 20 projektu), ochrony danych w fazie projektowania oraz ochrony danych jako opcji domyślnej (art. 23), a także prawo do bycia zapomnianym (art. 17). Celem tych prac jest znalezienie rozwiązań, które pozwolą na uzyskanie możliwie wysokiego poziomu ochrony danych osobowych obywateli i dostosowanie go do wymogów społeczeństwa informacyjnego, bez nadmiernego zwiększania obciążeń i kosztów po stronie przedsiębiorstw.

W odniesieniu do zgody na przetwarzanie danych, projekt rozporządzenia wzmacnia znaczenie zgody jako podstawy do przetwarzania danych osobowych. Z jednej strony zgoda powinna być udzielona w sposób wyraźny, nie powinna być milcząca czy dorozumiana z oświadczenia woli o innej treści, a także nie powinna stanowić podstawy przetwarzania danych osobowych w sytuacji wyraźnego braku równowagi pomiędzy podmiotem danych a administratorem. Jednak praktyczne stosowanie tego przepisu może okazać się uciążliwe dla internautów, zmuszonych do wyrażania zgody przy każdorazowym korzystaniu z nowej usługi. W związku z tym przedstawiciele biznesu opowiadają się za wprowadzeniem tzw. zgody kontekstowej, uzyskiwanej w oparciu o faktyczne działania podmiotu danych, a nie jedynie o jego wyrażne oświadczenie woli.

Przepis art. 20 projektu rozporządzenia dotyczący profilowania, dopuszcza profilowanie opierające się na automatycznym przetwarzaniu danych jedynie w ściśle określonych sytuacjach: w trakcie zawierania lub wykonywania umowy, gdy wyraźnie zezwala na to przepis prawa, lub po uzyskaniu zgody podmiotu danych. Przepis wprowadza również obowiązek poinformowania o tym osobę, która podlega poinformowaniu. Profilowanie co do zasady polega m.in. na zbieraniu danych o osobie z różnych źródeł, dzięki czemu powstaje obraz danej osoby, jej zachowań, preferencji konsumenckich, itd., ułatwiający dopasowanie kierowanych do niej reklam produktów i usług. Z drugiej jednak strony zachodzi obawa, że użytkownik może otrzymywać wyłącznie informacje

odpowiadające jego obecnym zainteresowaniom, zaś w przypadku niewłaściwego profilowania – zostaną mu zostać przypisane preferencje, które go nie dotyczą.

Z kolei art. 23 projektu rozporządzenia promuje zasady *privacy by design* i *privacy by default*. Oznacza to, że ustawienia ochrony prywatności w urządzeniach, produktach lub usługach powinny być maksymalnie ukierunkowane na ochronę użytkownika. Dzięki takiemu rozwiązaniu użytkownicy nie będą musieli przechodzić kolejnych etapów skomplikowanych ustawień, aby zapewnić najlepszą ochronę informacji na swój temat. Do użytkownika będzie też należała decyzja, czy i jakie dane o sobie chce udostępnić.

Natomiast wspomniany art. 17 projektowanego aktu zapewnia osobie, której dane dotyczą – przy spełnieniu określonych warunków – prawo do bycia zapomnianym i usunięcia dotyczących jej danych. Obecne brzmienie tego przepisu nakłada na administratora przetwarzającego dane osobowe – na wyraźne żądanie podmiotu danych – obowiązek usunięcia danych, poinformowania osób trzecich przetwarzających te dane o wniesionym żądaniu oraz usunięciu wszystkich linków do danych, kopii lub replikacji tych danych. Wspomniane prawo zapewniałoby z jednej strony ochronę danych osobowych podmiotu danych, ale z drugiej – informowanie każdego odbiorcy, któremu są ujawniane dane osobowe, o wszelkich operacjach ich poprawiania lub usunięcia, w praktyce jest operacją technicznie skomplikowaną i kosztowną do wprowadzenia. Ponadto definicja odbiorców jest tak szeroka, że zapis jest właściwie nie do zrealizowania i stanowić będzie ogromne obciążenie dla administratorów zbiorów danych, a w przestrzeni internetowej wręcz niemożliwy do realizacji. Opinię taką podziela organ do spraw ochrony danych osobowych, zaś Rząd RP w stanowisku do nowego rozporządzenia stwierdził wręcz, że obowiązek ten prawdopodobnie nie będzie wykonywany.

Prace nad projektem rozporządzenia toczyły się zarówno na forum Rady Unii Europejskiej, gdzie zasiadają przedstawiciele poszczególnych państw członkowskich (np. w ramach Grupy Roboczej Rady Unii Europejskiej ds. Wymiany Informacji i Ochrony Danych – DAPIX), jak i w Parlamencie Europejskim, w którym w 2012 r. odbyło się szereg głosowań nad tym dokumentem, na podstawie których wiodąca Komisja do spraw Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), podejmie w 2013 r. uchwałę o rekomendacjach w sprawie tego projektu. Dzięki wprowadzeniu nowych regulacji 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. Nowoczesne, spójne przepisy są niezbędne, aby mógł funkcjonować jednolity rynek, stymulujący rozwój gospodarczy, nowe miejsca pracy i wspierający innowacje. 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.

Natomiast zagadnienie **ochrony danych osobowych w ramach współpracy w sprawach karnych** było tematem diskutowanym od wielu lat. Zarówno dyrektywa 95/46/WE, jak i decyzja ramowa Rady 2008/977/WSiSW nie ma bowiem zastosowania do przetwarzania danych osobowych podejmowanej przez różne podmioty w ramach działalności wykraczającej poza zakres prawa Wspólnoty. Tymczasem przetwarzanie danych osobowych ma służyć człowiekowi, zaś zasady i przepisy je określające powinny – niezależnie od obywatelstwa czy miejsca zamieszkania osób fizycznych – respektować ich podstawowe prawa i wolności, w tym prawo do ochrony danych osobowych, przyczyniając się w ten sposób do stworzenia obszaru wolności, bezpieczeństwa i sprawiedliwości. W dobie szybkiego rozwoju technologicznego i globalizacji, gdzie gwałtownie wzrosła skala wymiany i zbierania danych, konieczne stało się stworzenie warunków ułatwiających swobodny przepływ danych między właściwymi organami na terytorium Unii oraz przekazywania danych do państw trzecich i organizacji międzynarodowych, przy równoczesnym zagwarantowaniu wysokiego poziomu ochrony danych osobowych. Stąd wniosek Parlamentu Europejskiego i Rady Unii Europejskiej o przyjęcie **dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania i ścigania**.

W odniesieniu do działalności informacyjno-edukacyjnej organu do spraw ochrony danych osobowych, na uwagę zasługuje nowa inicjatywa edukacyjna Generalnego Inspektora Ochrony Danych Osobowych organizowania konferencji, konsultacji i porad prawnych w ramach **Dni Otwartych GIODO w wybranych miejscowościach całej Polski**. W 2012 roku odbyły się dwa tego rodzaju przedsięwzięcia – w Dąbrowie Górniczej (22.11.2012 r.) i w Krakowie (23.11.2012 r.). Ciesząc się ogromnym zainteresowaniem Dni Otwarte GIODO, a także ciekawa formuła takich spotkań sprawiła, że już kolejne zaplanowane zostały na 2013 r. Ponadto w nadchodzącym 2013 roku Generalny Inspektor Ochrony Danych Osobowych będzie gospodarzem **35. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności**. Decyzję o przyznaniu Generalnemu Inspektorowi Ochrony Danych Osobowych GIODO statusu jej organizatora podjęto na 34. Konferencji Rzeczników Ochrony Danych i Prywatności, która miała miejsce w październiku 2012 r. w Urugwaju.

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 3 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 2012 o charakterze generalnym do centralnych organów państwa i do innych podmiotów  
z sektora publicznego**

<b>L.p.</b>	<b>Nazwa podmiotu, do którego skierowano wystąpienie</b>	<b>Data wystąpienia/ Sygnatura sprawy</b>	<b>Przedmiot wystąpienia</b>
1.	Minister Zdrowia	31.01.2012 DOLiS-035-2167/11	Wystąpienie o podjęcie prac legislacyjnych mających na celu przeniesienie regulacji zawartej w załączniku nr 3 pkt 2 oraz załączniku nr 4 pkt 4 do rozporządzenia Ministra Zdrowia z dnia 7 stycznia 2004 r. w sprawie badań lekarskich kierowców i osób ubiegających się o uprawnienia do kierowania pojazdami (Dz. U. z 2004 r. Nr 2, poz. 15, zm. Dz. U. z 2011 r. Nr 88, poz. 503) do aktu prawnego rangi ustawowej.
2.	Minister Edukacji Narodowej	13.02.2012 DOLiS-035-453/12	Prośba o podjęcie prac legislacyjnych mających na celu przeniesienie regulacji zawartych w rozporządzeniu Ministra Edukacji Narodowej z dnia 27 października 2009 r. w sprawie wymagań, jakim powinna odpowiadać osoba zajmująca stanowisko dyrektora oraz inne stanowisko kierownicze w poszczególnych typach publicznych szkół i rodzajach publicznych placówek (Dz. U. z 2009 r. Nr 184, poz. 1436) do aktu prawnego rangi ustawowej.
3.	Polska Izba Ubezpieczonych	17.02.2012 DOLiS-035-522/12	Prośba o podjęcie stosownych kroków w celu unaocznienia zakładom ubezpieczeń możliwości naruszenia przepisów o ochronie danych osobowych, które może mieć miejsce poprzez stosowanie praktyki polegającej na dopisywaniu w tytułach przelewów (np. z tytułu świadczenia umowy ubezpieczenia) dodatkowych informacji, w szczególności o charakterze danych szczególnie chronionych, identyfikujących przyczynę wypłaty odszkodowania.
4.	Minister Zdrowia	6.03.2012 DOLiS-035-637/12	Prośba o podjęcie prac legislacyjnych mających na celu określenie jednolitego wzoru legitymacji Honorowego Dawcy Krwi, ze szczególnym uwzględnieniem zakresu zawartych w tym dokumencie informacji, co pozwoli na wyeliminowanie problemu często nadmiernej i niejednokrotnie zbędnej ingerencji w prywatność osób oddających krew, Honorowych Dawców Krwi.
5.	Minister Transportu, Budownictwa i Gospodarki Morskiej	23.03.2012 DOLiS-035-880/12	Prośba o podjęcie prac legislacyjnych w celu zmiany art. 16 ust. 3 ustawy z dnia 15 listopada 1984 r. Prawo przewozowe (Dz. U. z 2000 r. Nr 50, poz. 601 z późn. zm.) dotyczącego zakresu danych osobowych, jaki może być umieszczony na bilecie, stanowiącym potwierdzenie zwarcia umowy przewozu.
			Prośba o podjęcie prac legislacyjnych mających na

6.	Minister Pracy i Polityki Społecznej	23.03.2012 DOLiS-035-893/12	celu prawne uregulowanie zasad i sposobu prowadzenia dokumentacji przez psychologów.
7.	Minister Zdrowia	27.03.2012 DOLiS-035- 995/12	Wystąpienie w sprawie wyeliminowania praktyki umieszczania przy łóżkach pacjentów kart gorączkowych.
8.	Minister Sprawiedliwości	2.04.2012 DOLiS-035-993/12	Prośba o podjęcie prac legislacyjnych mających na celu prawne uregulowanie zasad i sposobu prowadzenia dokumentacji przez rodzinne ośrodki diagnostyczne-konsultacyjne.
9.	Minister Rolnictwa i Rozwoju Wsi	12.04.2012 DOLiS-035-327/12	Prośba o podjęcie działań legislacyjnych celem zmiany aktualnego stanu prawnego wynikającego z przepisów art. 23c ust. 3 ustawy z dnia 26 czerwca 2003 r. o ochronie prawnej odmian roślin (Dz. U. Nr 137, poz. 1300 z późn. zm.).
10.	Naczelna Rada Lekarska	17.04.2012 DOLiS-035-1188/12	Prośba o zasygnalizowanie członkom samorządu lekarskiego konieczności respektowania prawa do prywatności oraz ochrony informacji związanych z pacjentem podczas wykonywania praktyk lekarskich, jak również organizowania obsługi pacjentów, w szczególności w sytuacjach rejestrowania pacjentów na wizyty lekarskie, wydawania im wyników badań, ustalania harmonogramu zabiegów w sanatoriach, wywoływania do gabinetów lekarskich lekarzy specjalistów
11.	Rada m.st. Warszawy	23.04.2012 DIS-K-421/182/11/25913/12	Podjęcie działań mających na celu zmianę taryfy przewozowej w zakresie zapisu dotyczącego obowiązku okazywania dokumentu tożsamości przez osoby zwracające bilety.
12.	Minister Zdrowia	12.06.2012 DOLiS-035-1669/12	Prośba o podjęcie prac legislacyjnych mających na celu wprowadzenie ustawowych podstaw prawnych dla przekazywania danych osobowych uczniów podmiotom prowadzącym działalność leczniczą, w związku z realizacją umów w ramach profilaktycznej opieki zdrowotnej nad dziećmi i młodzieżą.
13.	Przewodniczący Komisji Nadzoru Finansowego	17.07.2012 DIS-424/44035/12	Podjęcie działań zmierzających do zwrócenia uwagi bankom spółdzielczym i bankom zrzeszającym, na konieczność dostosowania procesu przetwarzania danych osobowych do wymogów ustawy o ochronie danych osobowych, polegających na obowiązku uaktualniania bez zbędnej zwłoki, danych osobowych ich klientów przekazywanych Biuru Informacji Kredytowej.



## Wykaz kontroli przeprowadzonych w 2012 r.

L.p.	Sygnatura kontroli	Nazwa i siedziba podmiotu kontrolowanego	Rozstrzygnięcie
1.	DIS-K-421/2/12	Przedszkole nr 414, Warszawa, ul. Ostródzka 175d	decyzja GODO
2.	DIS-K-421/3/12	Przedszkole nr 76, Warszawa, ul. Odkryta 18	nie stwierdzono uchybień
3.	DIS-K-421/4/12	Prezydent m.st. Warszawy – Biuro Edukacji m.st. Warszawy, Warszawa, ul. W. Górskiego 7	nie stwierdzono uchybień
4.	DIS-K-421/1/12	Przedszkole Samorządowe nr 1 „Pod Topolą”, Bełchatów, ul. 1 Maja 4a	decyzja GODO
5.	DIS-K-421/5/12	Konsalnet Konwój Sp. z o.o., Warszawa, ul. Przasnyska 6a	decyzja GODO
6.	DIS-K-421/6/12	World Class Health Academy Polska Sp. z o.o. Warszawa, Al. Jerozolimskie 65/79	decyzja GODO
7.	DIS-K-421/7/12	Bank Polskiej Spółdzielczości S.A., Warszawa, ul. Płocka 9/11B	nie stwierdzono uchybień
8.	DIS-K-421/8/12	SGB-Bank S.A., Poznań, ul. Szarych Szeregów 23A	nie stwierdzono uchybień
9.	DIS-K-421/9/12	Bank Spółdzielczy w Legionowie, Legionowo, ul. Rynek 4	nie stwierdzono uchybień
10.	DIS-K-421/10/12	Warszawski Bank Spółdzielczy, Warszawa, ul. Fieldorfa 5A	nie stwierdzono uchybień
11.	DIS-K-421/11/12	Maciej Jackowiak prowadzący działalność gospodarczą pod nazwą „Prywatny Gabinet Lekarski Jackowiak Maciej”, Toruń, ul. Broniewskiego 4/2	przywrócono stan zgodny z prawem
12.	DIS-K-421/12/12	Zakład Usług Informatycznych OTAGO Sp. z o.o., Kraków, ul. Lea 114/6	nie stwierdzono uchybień
13.	DIS-K-421/13/12	Polski Holding Nieruchomości S.A., Warszawa, ul. Świętokrzyska 36	wykonano decyzję GODO
14.	DIS-K-421/19/12	Janina Bartkiewicz prowadząca działalność gospodarczą pod nazwą „MIRJAN”, Warszawa, Al. Szucha 2/4 lok. 50	decyzja GODO
15.	DIS-K-421/14/12	PSI Pharma Support Poland Sp. z o.o. Warszawa, ul. 1-go Sierpnia 6a	decyzja GODO
16.	DIS-K-421/18/12	Główny Geodeta Kraju – Główny Urząd Geodezji i Katastru, Warszawa, ul. Wspólna 2	nie stwierdzono uchybień
17.	DIS-K-421/15/12	Polski Bank Spółdzielczy w Wyszkowie, Wyszków, ul. Kościuszki 5	nie stwierdzono uchybień
18.	DIS-K-421/16/12	Sąd Okręgowy Warszawa - Praga, Warszawa, Al. Solidarności 127	nie stwierdzono uchybień
19.	DIS-K-421/17/12	Sąd Okręgowy w Warszawie, Warszawa, Al. Solidarności 127	nie stwierdzono uchybień
20.	DIS-K-421/22/12	Znany Lekarz Sp. z o.o., Warszawa, ul. Bitwy Warszawskiej 1920 r. 7	decyzja GODO
21.	DIS-K-421/20/12	Bank Spółdzielczy w Nowym Dworze Maz. Nowy Dwór Mazowiecki, ul. Słowackiego 8	przywrócono stan zgodny z prawem
22.	DIS-K-421/21/12	Bank Spółdzielczy w Pruszkowie, Pruszków, ul. Prusa 88	nie stwierdzono uchybień
23.	DIS-K-421/24/12	Groupon Sp. z o.o., Warszawa, Al. Jerozolimskie 123A	decyzja GODO
24.	DIS-K-421/23/12	Sąd Okręgowy w Katowicach, Katowice, ul. Francuska 38	nie stwierdzono uchybień
25.	DIS-K-421/25/12	Poznański Bank Spółdzielczy, Poznań, ul. Głogowska 47/47a	nie stwierdzono uchybień
26.	DIS-K-421/27/12	Miejski Ośrodek Sportu i Rekreacji,	nie stwierdzono uchybień

		Toruń, ul. Bema 23/29	
27.	DIS-K-421/26/12	Prokuratura Okręgowa Warszawa – Praga, Warszawa, ul. Bródnowska 13/15	nie stwierdzono uchybień
28.	DIS-K-421/28/12	Bank Spółdzielczy w Skierniewicach, Skierniewice, ul. Reymonta 25	nie stwierdzono uchybień
29.	DIS-K-421/30/12	Violetta Stasiewicz i Mariusz Stasiewicz, wspólnicy „Halma” s.c. Wrocław, ul. Metalowców 25	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
30.	DIS-K-421/29/12	Niepubliczne Przedszkole „Chatka Puchatka”, Legionowo, ul. Sienkiewicza 6	nie stwierdzono uchybień
31.	DIS-K-421/31/12	Business Zone Sp. z o.o. Warszawa, ul. Chałbińskiego 8	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
32.	DIS-K-421/35/12	BNT Neupert Zamorska & Partnerzy sp.j. Warszawa, ul. Krakowskie Przedmieście 47/51	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
33.	DIS-K-421/32/12	Niepubliczne Przedszkole „Kleks”, Piaseczno, ul. Jana Pawła II 36	nie stwierdzono uchybień
34.	DIS-K-421/33/12	Prokuratura Okręgowa w Gliwicach, Gliwice, ul. Dubois 16	nie stwierdzono uchybień
35.	DIS-K-421/34/12	Prokuratura Okręgowa w Warszawie, Warszawa, ul. Chocimska 28	przywrócono stan zgodny z prawem
36.	DIS-K-421/36/12	Przedszkole nr 55, Warszawa, ul. Jana Cybisa 1	decyzja GODO
37.	DIS-K-421/37/12	Krakowski Bank Spółdzielczy, Kraków, ul. Rynek Kleparski 8	nie stwierdzono uchybień
38.	DIS-K-421/38/12	Powiatowy Urząd Pracy, Piotrków Trybunalski, ul. Dmowskiego 27	nie stwierdzono uchybień
39.	DIS-K-421/39/12	Bank Spółdzielczy Rzemiosła, Kraków, ul. Dunajewskiego 7	nie stwierdzono uchybień
40.	DIS-K-421/40/12	Dariusz Socik prowadzący działalność gospodarczą pod nazwą „Interrete Dariusz Socik”, Warszawa, ul. Chodkiewicza 10/51	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
41.	DIS-K-421/41/12	Klub Piłkarski Legia Warszawa S.S.A. Warszawa, ul. Łazienkowska 3	decyzja GODO
42.	DIS-K-421/42/12	Hotele Warszawskie „Syrena” Sp. z o.o. Warszawa, Pl. Konstytucji 1	nie stwierdzono uchybień
43.	DIS-K-421/44/12	Neohause Sp. z o.o. Warszawa, ul. Mokotowska 12	decyzja GODO
44.	DIS-K-421/45/12	LIM Joint Venture Sp. z o.o. Warszawa, Al. Jerozolimskie 65/79	decyzja GODO
45.	DIS-K-421/46/12	Hotele Korona Sp. z o.o. Warszawa, ul. Majdańska 1	decyzja GODO
46.	DIS-K-421/47/12	Piotr Toporkiewicz prowadzący działalność gospodarczą pod nazwą „FHU COPIT Piotr Toporkiewicz”, Gliwice, ul. Centaura 7/6	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
47.	DIS-K-421/48/12	Okręgowy Zarząd Łódzki Polskiego Związku Działkowców, Łódź, ul. Warecka 3	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
48.	DIS-K-421/49/12	Fundacja Praworządni.pl, Warszawa, ul. Nowoursynowska 160A/5	w toku
49.	DIS-K-421/50/12	Royal Starman Bristol Sp. z o.o. Warszawa, ul. Krakowskie Przedmieście 42/44	decyzja GODO
50.	DIS-K-421/53/12	Adesco Sp. z o.o. Lublin, ul. Mełgiewska 11	brak przetwarzania danych osobowych w zakresie objętym kontrolą
51.	DIS-K-421/55/12	Hotel LOGOS Filia Oddziału Usług Pedagogicznych i Socjalnych ZNP, Warszawa, ul. Wybrzeże Kościuszkowskie 31/33	decyzja GODO
52.	DIS-K-421/51/12	Hekon Hotele Ekonomiczne S.A. Kraków, ul. Syrokomli 2	nie stwierdzono uchybień
53.	DIS-K-421/52/12	UBM HPG Sp. z o.o. Kraków, ul. Krupnicza 16	decyzja GODO
54.	DIS-K-421/54/12	Powiatowy Urząd Pracy	nie stwierdzono uchybień

		w Siemianowicach Śląskich Siemianowice Śląskie, ul. Wyzwolenia 17	
55.	DIS-K-421/56/12	Hotel G.E. Towarowa Warszawa Sp. z o.o. Warszawa, ul. Nowogrodzka 21	decyzja GODO
56.	DIS-K-421/57/12	Związek Harcerstwa Polskiego Warszawa, ul. Konopnickiej 6	decyzja GODO
57.	DIS-K-421/58/12	Data Connect Sp. z o.o. Toruń, ul. Wielkie Garbary 7a	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
58.	DIS-K-421/59/12	Soccer Skills Sp. z o.o. Warszawa, Al. Jerozolimskie 125/127 lok. 209	decyzja GODO
59.	DIS-K-421/61/12	Lexis Polska Sp. z o.o. Wrocław, ul. Pilczycka 201	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
60.	DIS-K-421/62/12	Dwór Oliwski Sp. z o.o. Gdańsk, ul. Bytowska 4	decyzja GODO
61.	DIS-K-421/63/12	Politechnika Gdańska, Gdańsk, ul. Narutowicza 11/12	nie stwierdzono uchybień
62.	DIS-K-421/64/12	Prezydent Miasta Gdańska – Urząd Miejski w Gdańsku, Gdańsk, ul. Nowe Ogrody 8/12	brak przetwarzania danych osobowych w zakresie objętym kontrolą
63.	DIS-K-421/65/12	Prezydent Miasta Białystok – Urząd Miasta Białystok, Białystok, ul. Słonimska 1	nie stwierdzono uchybień
64.	DIS-K-421/66/12	Orbis S.A. Warszawa, ul. Bracka 16	decyzja GODO
65.	DIS-K-421/67/12	Holding Liwa Sp. z o.o. Wrocław, ul. Modrzejewskiej 2	nie stwierdzono uchybień
66.	DIS-K-421/69/12	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
67.	DIS-K-421/70/12	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
68.	DIS-K-421/72/12	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
69.	DIS-K-421/68/12	Piotr Gurba i Tomasz Palusiński prowadzący działalność gospodarczą pod nazwą „Prorider Polska”, Świeradów Zdrój, ul. Źródlana 7	nie stwierdzono uchybień
70.	DIS-K-421/60/12	Halcash Central Eastern Europe Sp. z o.o. Warszawa, ul. Rejtana 17 lok. 23	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
71.	DIS-K-421/73/12	CT Creative Team S.A. Warszawa, ul. Chałbińskiego 8	nie stwierdzono uchybień
72.	DIS-K-421/74/12	Firm.Info Sp. z o.o. Warszawa, ul. Ogrodowa 28/30 lok. 407	nie stwierdzono uchybień
73.	DIS-K-421/75/12	Fundacja „Przeciwko Leukemii” Warszawa, ul. Morcinka 5/19	nie stwierdzono uchybień
74.	DIS-K-421/77/12	Polska Telefonii Komórkowa Centertel Sp. z o.o. Warszawa, ul. Skierniewicka 10A	nie stwierdzono uchybień
75.	DIS-K-421/76/12	Wojskowy Instytut Medyczny Warszawa, ul. Szaserów 128	przywrócono stan zgodny z prawem
76.	DIS-K-421/78/12	Alior Bank S.A. Warszawa, Al. Jerozolimskie 94	nie stwierdzono uchybień
77.	DIS-K-421/79/12	Fundacja Praworządni.pl Warszawa, ul. Nowoursynowska 160A/5	w toku
78.	DIS-K-421/82/12	Arkadiusz Ozga prowadzący działalność gospodarczą pod nazwą „Global Finance Arkadiusz Ozga” Częstochowa, ul. Kiedrzyńska 38	nie stwierdzono uchybień
79.	DIS-K-421/80/12	Bartosz Bąk prowadzący działalność gospodarczą pod nazwą „szybkopewnie.pl”, Lublin, ul. Zana 10/63	decyzja GODO
80.	DIS-K-421/81/12	Instytut Hematologii i Transfuzjologii, Warszawa, ul. Indiry Gandhi 14	decyzja GODO
81.	DIS-K-421/83/12	LIM Joint Venture Sp. z o.o. Warszawa, Al. Jerozolimskie 65/79	decyzja GODO
82.	DIS-K-421/84/12	Polskie Linie Lotnicze „LOT”	decyzja GODO

		Warszawa, ul. 17 stycznia 39	
83.	DIS-K-421/85/12	Prezydent Miasta Wrocławia – Urząd Miasta Wrocławia, Wrocław, Pl. Nowy Targ 1-8	nie stwierdzono uchybień
84.	DIS-K-421/88/12	Aldi Sp. z o.o. Chorzów, ul. Niedźwiedziniec 10	decyzja GODO
85.	DIS-K-421/89/12	Burmistrz Dzielnicy Ursynów m.st. Warszawy – Urząd Dzielnicy Ursynów Warszawa, ul. KEN 61	nie stwierdzono uchybień
86.	DIS-K-421/87/12	Krajowy Rejestr Pracowników i Pracodawców, Grudziądz, ul. Legionów 3	nie stwierdzono uchybień
87.	DIS-K-421/90/12	Miejski Ośrodek Pomocy Rodzinie Piotrków Trybunalski, ul. Próchnika 34	decyzja GODO
88.	DIS-K-421/91/12	Miejski Ośrodek Pomocy Rodzinie Sulejów, ul. Targowa 20	decyzja GODO
89.	DIS-K-421/92/12	DKMS Baza Dawców Komórek Macierzystych Warszawa, ul. Altowa 18	decyzja GODO
90.	DIS-K-421/93/12	Centrum Krwiodawstwa i Krwiolecznictwa – Samodzielny Publiczny Zakład Opieki Zdrowotnej, Lublin, ul. Armii Wojska Polskiego 8	nie stwierdzono uchybień
91.	DIS-K-421/95/12	Konsalnet Ochrona Sp. z o.o. Warszawa, ul. Przasnyska 6a	decyzja GODO
92.	DIS-K-421/97/12	Regionalne Centrum Krwiodawstwa i Krwiolecznictwa, Warszawa, ul. Saska 63/75	nie stwierdzono uchybień
93.	DIS-K-421/96/12	Centrum Krwiodawstwa i Krwiolecznictwa – Samodzielny Publiczny Zakład Opieki Zdrowotnej, Białystok, ul. Skłodowskiej – Curie 23	nie stwierdzono uchybień
94.	DIS-K-421/98/12	Podlaski Oddział Straży Granicznej Białystok, ul. Bema 100	nie stwierdzono uchybień
95.	DIS-K-421/99/12	Śląski Oddział Straży Granicznej Racibórz, ul. Dąbrowskiego 2A	nie stwierdzono uchybień
96.	DIS-K-421/101/12	Bull Polska Sp. z o.o. Warszawa, ul. Królewska 16	nie stwierdzono uchybień
97.	DIS-K-421/100/12	Placówka Straży Granicznej Warszawa – Modlin Nowy Dwór Mazowiecki, ul. Thommee 1a	nie stwierdzono uchybień
98.	DIS-K-421/103/12	Galiczyjskie Centrum Edukacji Sp. z o.o. Kraków, ul. Bronowicka 73	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
99.	DIS-K-421/102/12	SP ZOZ Centralny Szpital Kliniczny Instytutu Stomatologii Uniwersytetu Medycznego w Łodzi Łódź, ul. Pomorska 251	nie stwierdzono uchybień
100.	DIS-K-421/106/12	Biuro Informacji Kredytowej S.A. Warszawa, ul. Mokotowska 19	nie stwierdzono uchybień
101.	DIS-K-421/104/12	Elżbieta Olszak prowadząca działalność gospodarczą pod nazwą „Elżbieta Olszak Ośrodek Szkolenia Kursowego i Ustawicznego” Kraków, ul. Bronowicka 73	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
102.	DIS-K-421/105/12	BRE Bank S.A. Warszawa, ul. Senatorska 18	decyzja GODO
103.	DIS-K-421/110/12	Zarząd Transportu Miejskiego Warszawa, ul. Żelazna 61	nie stwierdzono uchybień
104.	DIS-K-421/107/12	Placówka Straży Granicznej Warszawa – Okęcie Warszawa, ul. 17 stycznia 45D	nie stwierdzono uchybień
105.	DIS-K-421/108/12	Wojewódzki Urząd Pracy w Zielonej Górze Zielona Góra, ul. Wyspiańskiego 15	nie stwierdzono uchybień
106.	DIS-K-421/109/12	Regionalne Centrum Krwiodawstwa i Krwiolecznictwa w Poznaniu Poznań, ul. Marcelińska 44	decyzja GODO
107.	DIS-K-421/111/12	Straż Miejska m.st. Warszawy Warszawa, ul. Młynarska 43/45	nie stwierdzono uchybień
108.	DIS-K-421/112/12	Wyższa Szkoła Menedżerska Warszawa, ul. Kawęczyńska 36	nie stwierdzono uchybień
109.	DIS-K-421/113/12	Alitalia – Compagnia Aera Italiana S.P.A.S.A.	wnioski przekazano do Departamentu

		Oddział w Polsce, Warszawa, ul. Nowy Świat 64	Orzecznictwa Legislacji i Skarg
110.	DIS-K-421/114/12	Korona S.A., Kielce, ul. Ściegiennego 8	nie stwierdzono uchybień
111.	DIS-K-421/115/12	Warszawska Szkoła Filmowa Warszawa, ul. Zajęczka 7	decyzja GODO
112.	DIS-K-421/116/12	Wojewoda Małopolski – Małopolski Urząd Wojewódzki w Krakowie Kraków, ul. Basztowa 22	nie stwierdzono uchybień
113.	DIS-K-421/117/12	Polska Telefonía Cyfrowa S.A. Warszawa, Al. Jerozolimskie 181	nie stwierdzono uchybień
114.	DIS-K-421/118/12	Wojewoda Mazowiecki – Mazowiecki Urząd Wojewódzki, Warszawa, Pl. Bankowy 3/5	przywrócono stan zgodny z prawem
115.	DIS-K-421/123/12	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
116.	DIS-K-421/119/12	Akademia Sztuk Pięknych im. W. Strzemińskiego Łódź, ul. Wojska Polskiego 121	nie stwierdzono uchybień
117.	DIS-K-421/120/12	Nextbike Polska Sp. z o.o. Wrocław, ul. Kruszwicka 26/28	nie stwierdzono uchybień
118.	DIS-K-421/121/12	Komendant Główny Straży Granicznej Warszawa, Al. Niepodległości 100	nie stwierdzono uchybień
119.	DIS-K-421/122/12	Akademia Górniczo – Hutnicza im. St. Staszica Kraków, Al. Mickiewicza 30	decyzja GODO
120.	DIS-K-421/124/12	Wojewoda Warmińsko – Mazurski Olsztyn, Al. Piłsudskiego 7/9	nie stwierdzono uchybień
121.	DIS-K-421/125/12	Netia S.A., Warszawa, ul. Poleczki 13	nie stwierdzono uchybień
122.	DIS-K-421/126/12	Polkomtel Sp. z o.o., Warszawa, ul. Postępu 3	nie stwierdzono uchybień
123.	DIS-K-421/127/12	Telekomunikacja Novum S.A. Warszawa, Raclawicka 146	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
124.	DIS-K-421/128/12	Lingwistyczna Szkoła Wyższa Warszawa, ul. Żelazna 87	nie stwierdzono uchybień
125.	DIS-K-421/129/12	Politechnika Warszawska Warszawa, Pl. Politechniki 1	decyzja GODO
126.	DIS-K-421/130/12	Agnieszka Klimaszewska – Zapała prowadząca działalność gospodarczą pod nazwą „Usługi Biurowo – Kadrowe Firm Agnieszka Klimaszewska – Zapała”, Kielce, ul. Bukowa 6/26	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
127.	DIS-K-421/135/12	Centrum Organizacyjno – Koordynacyjne do Spraw Transplantacji „Poltransplant” Warszawa, Al. Jerozolimskie 87	nie stwierdzono uchybień
128.	DIS-K-421/131/12	Wyższa Szkoła Finansów i Zarządzania Białystok, ul. Ciepła 40	nie stwierdzono uchybień
129.	DIS-K-421/132/12	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	nie stwierdzono uchybień
130.	DIS-K-421/133/12	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
131.	DIS-K-421/134/12	Grono.net S.A., Warszawa, ul. Jelinka 32	decyzja GODO
132.	DIS-K-421/136/12	Uniwersytet Mikołaja Kopernika w Toruniu Toruń, ul. Gagarina 11	nie stwierdzono uchybień
133.	DIS-K-421/137/12	Legg Mason Towarzystwo Funduszy Inwestycyjnych S.A. Warszawa, Pl. Piłsudskiego 2	decyzja GODO
134.	DIS-K-421/138/12	SP ZOZ Ministerstwa Spraw Wewnętrznych – Warmińsko – Mazurskie Centrum Onkologii Olsztyn, ul. Wojska Polskiego 37	nie stwierdzono uchybień
135.	DIS-K-421/139/12	Paycash Services Sp. z o.o. Warszawa, ul. Rejtana 17	nie stwierdzono uchybień
136.	DIS-K-421/140/12	Wspólnota Mieszkaniowa Łódź, Al. Śmigłego – Rydza 84	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
137.	DIS-K-421/141/12	Towarzystwo Ubezpieczeń Allianz Życie Polska S.A., Warszawa, ul. Rodziny Hiszpańskich 1	nie stwierdzono uchybień
138.	DIS-K-421/142/12	BEST S.A., Gdynia, ul. Morska 59	nie stwierdzono uchybień
139.	DIS-K-421/143/12	Polska Telefonía Komórkowa Centertel	nie stwierdzono uchybień

		Sp. z o.o., Warszawa, ul. Skierniewicka 10A	
140.	DIS-K-421/144/12	Ministerstwo Nauki i Szkolnictwa Wyższego Warszawa, ul. Wspólna 1/3	decyzja GODO
141.	DIS-K-421/147/12	Konsalnet Holding S.A. Warszawa, ul. Przasnyska 6A	decyzja GODO
142.	DIS-K-421/145/12	Liceum Plastyczne im. Kossaka Łomża, ul. Skłodowskiej – Curie 1	przywrócono stan zgodny z prawem
143.	DIS-K-421/146/12	Ogólnopolski Rejestr Danych Osobowych Sp. z o.o., Warszawa, ul. Królowej Marysieńki 20 lok. 2	decyzja GODO
144.	DIS-K-421/145/12	Minister Pracy i Polityki Społecznej Warszawa, ul. Nowogrodzka 1/3/5	usunięto uchybienia
145.	DIS-K-421/149/12	Naczelna Izba Lekarska Warszawa, ul. Sobieskiego 110	nie stwierdzono uchybień
146.	DIS-K-421/150/12	I Liceum Ogólnokształcące im. Kopernika Łódź, ul. Więckowskiego 41	nie stwierdzono uchybień
147.	DIS-K-421/151/12	Wojskowa Prokuratura Okręgowa Warszawa, ul. Nowowiejska 26B	przywrócono stan zgodny z prawem
148.	DIS-K-421/152/12	Hotel Reservation Services Poland Sp. z o.o., Warszawa, Al. Jana Pawła II 19	nie stwierdzono uchybień
149.	DIS-K-421/155/12	Firm.Info Sp. z o.o. Warszawa, ul. Ogrodowa 28/30 lok. 407	nie stwierdzono uchybień
150.	DIS-K-421/153/12	Prezes Głównego Urzędu Statystycznego Warszawa, Al. Niepodległości 208	decyzja GODO
151.	DIS-K-421/154/12	Agencja Nasienna Sp. z o.o. Leszno, ul. Jana Dekana 6E	decyzja GODO
152.	DIS-K-421/156/12	Alan Systems Sp. z o.o. sp. k., Rybnik, ul. Obwiednia Południowa 22	nie stwierdzono uchybień
153.	DIS-K-421/159/12	Netia S.A., Warszawa, ul. Poleczki 13	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
154.	DIS-K-421/157/12	Wydział Konsularny Ambasady RP w Republice Federalnej Niemiec Berlin, Lassenstr. 19-21	nie stwierdzono uchybień
155.	DIS-K-421/161/12	Ośrodek Przetwarzania Informacji Instytut Badawczy Warszawa, Al. Niepodległości 188B	nie stwierdzono uchybień
156.	DIS-K-421/162/12	Sygnity S.A. Warszawa, Al. Jerozolimskie 180	nie stwierdzono uchybień
157.	DIS-K-421/163/12	IAI S.A., Szczecin, ul. Madalińskiego 8	decyzja GODO
158.	DIS-K-421/166/12	Ośrodek Przetwarzania Informacji Instytut Badawczy Warszawa, Al. Niepodległości 188B	usunięto uchybienia
159.	DIS-K-421/164/12	Barbara Ordyk prowadząca działalność gospodarczą pod nazwą „Wydawnictwo Ambrozja Barbara Ordyk” Kraków, ul. Łobzowska 55 lok. 10	nie stwierdzono uchybień
160.	DIS-K-421/165/12	Wydział Konsularny Ambasady RP w Republice Czeskiej Praga, ul. Valdstejska 8	nie stwierdzono uchybień
161.	DIS-K-421/167/12	Centralny Organ Techniczny KSI (Komendant Główny Policji), Warszawa, ul. Puławska 148/150	nie stwierdzono uchybień
162.	DIS-K-421/171/12	Edyta Wieloch – Górska i Maciej Frontczak prowadzący działalność gospodarczą pod nazwą „Vista Vision s.c.”, Kalisz, ul. Graniczna 21	zaprzesano prowadzenia działalności gospodarczej
163.	DIS-K-421/170/12	Kamil Kornak prowadzący działalność gospodarczą pod nazwą „Kuplaptopa.pl”, Warszawa, Al. Jerozolimskie 123A	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
164.	DIS-K-421/168/12	Bank Millenium S.A., Warszawa, ul. Żaryna 2A	nie stwierdzono uchybień
165.	DIS-K-421/169/12	4 Health Group Dąbrowski Sp.k. Katowice, ul. Opolska 11/3	decyzja GODO

**Wykaz orzeczeń wydanych w 2012 r. przez  
Wojewódzki Sąd Administracyjny w Warszawie i Naczelny Sąd Administracyjny  
w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych**

<b>L.p.</b>	<b>Data/ sygnatura orzeczenia WSA w Warszawie lub NSA</b>	<b>Sygnatura rozstrzygnięcia GIODO</b>	<b>Przedmiot sprawy</b>	<b>Rozstrzygnięcie WSA w Warszawie lub NSA</b>
1.	05.01.2012 II SA/Wa 2659/11	DOLiS/DEC- 888/11/50721, 50726	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
2.	11.01.2012 II SA/Wa 1582/11	DOLiS-440-429/10	Wniosek o przywrócenie terminu do zgłoszenia wniosku o sporządzenie uzasadnienia wyroku WSA z dnia 14 grudnia 2011 r.	odmowa przywrócenia terminu
3.	12.01.2012 I OSK 2385/11	DOLiS/POST- 75/11/ 14847, 14849,14851	Skarga na postanowienie w przedmiocie uzupełnienia decyzji	ddalenie skargi kasacyjnej
4.	18.01.2012 II SAB/Wa 486/11	DOLiS-440-200/07	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	oddalenie skargi
5.	24.01.2012 II SA/Wa 1940/11	DIS/DEC- 505/29532/11	Opcjonalność wyrażenia zgody na przetwarzanie danych osobowych	umorzenie postępowania
6.	27.01.2012 II SA/Wa 2069/11	DOLiS/DEC- 604/11/35410, 35412	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
7.	31.01.2012 II SAB/Wa 173/11	DOLiS-440-119/11	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	uzupełnienie postanowienia WSA w Warszawie z dnia 12.10.2011 r.
8.	31.01.2012 I OSK 1317/11	DOLiS/DEC- 1312/10/47293	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi kasacyjnej
9.	02.02.2012 II SA/Wa 2333/11	DOLiS/DEC- 718/11/40245, 40249	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
10.	08.02.2012 II SAB/Wa 412/11	DOLiS-440-185/10	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	oddalenie skargi
11.	17.02.2012 I OZ 88/12	GI-DEC-DS.- 380/05/1067,1068, 1069	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonego zarządzenia i odrzucenie wniosku o przywrócenie terminu do wniesienia skargi kasacyjnej
12.	23.02.2012 II SA/Wa 2466/11	DOLiS/POST- 191/11/41144, 41145,41146	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku o wydanie kserokopii akt sprawy	oddalenie skargi
13.	27.02.2012 II SAB/Wa 61/12	DOLiS-440- 1046/09	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	oddalenie skargi
14.	27.02.2012 II SA/Wa 9/12	DOLiS/POST- 41/10/8991,8992, 8994,8995,8996	Skarga na postanowienie w przedmiocie odmowy sporządzenia i przesłania uwierzytelnionych kserokopii dokumentów z akt sprawy	oddalenie skargi
15.	27.02.2012 II SA/Wa 2848/11	DOLiS/DEC- 531/10/17993,	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi

		17996,18002,18008, 18015		
16.	29.02.2012 I OZ 99/12	DOLiS/POST- 191/11/41144, 41145,41146	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku o wydanie kserokopii akt sprawy	oddalenie zażalenia
17.	05.03.2012 II SA/Wa 2814/11	DOLiS/DEC- 890/11/50743, 50747,50750, 50751,50752	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
18.	06.03.2012 II SA/Wa 2235/11	DOLiS/DEC- 632/11/35872, 35874/11	Skarga na decyzję w przedmiocie umorzenia postępowania	oddalenie skargi
19.	13.03.2012 II SAB/Wa 59/12	DOLiS-440-976/09	Skarga na bezczynność w przedmiocie ochrony danych osobowych	oddalenie skargi
20.	19.03.2012 II SA/Wa 2399/11	DOLiS/DEC- 710/11/40217, 40220	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
21.	20.03.2012 II SA/Wa 2765/11	DOLiS-067-30/11	Skarga w przedmiocie dostępu do informacji publicznej	oddalenie skargi
22.	27.03.2012 I OZ 192/12	DOLiS-440-119/11	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	uchylenie zaskarżonego postanowienia w części dotyczącej zwrotu kosztów postępowania
23.	27.03.2012 I OZ 194/12	DOLiS-440-151/11	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	uchylenie zaskarżonego postanowienia w punkcie drugim
24.	27.03.2012 II SA/Wa 215/12	DOLiS-035- 3234/11	Skarga na pismo GIODO w przedmiocie ochrony danych osobowych	oddalenie skargi
25.	29.03.2012 II SA/Wa 152/12	DOLiS-440- 711/08/10775/10	Skarga na pismo GIODO w przedmiocie ochrony danych osobowych	oddalenie skargi
26.	30.03.2012 II SAB/Wa 484/11	DOLiS-440-714/09	Skarga na bezczynność w przedmiocie rozpatrzenia skargi	umorzenie postępowania
27.	03.04.2012 II SA/Wa 1582/11	DOLiS/DEC- 450/11/26448, 26449	Skarga na decyzję GIODO w przedmiocie nakazu udostępnienia danych osobowych w zakresie imienia, nazwiska oraz adresu zameldowania	odmowa sporządzenia uzasadnienia wyroku
28.	03.04.2012 II SA/Wa 165/12	DOLiS/DEC- 1011/11/57732,577 35,57737	Skarga na decyzję GIODO w przedmiocie ochrony danych osobowych	oddalenie skargi
29.	04.04.2012 II SA/Wa 154/12	DOLiS-440- 711/08/10775/10	Skarga na pismo GIODO w przedmiocie ochrony danych osobowych	sprostowanie z urzędu oczywistej omyłki pisarskiej
30.	12.04.2012 II SA/Wa 2826/11	DIS/DEC- 900/51667/11	Usunięcie z urzędu densytometrycznego danych osobowych skarżącego	uchylenie zaskarżonej decyzji
31.	16.04.2012 II SA/Wa 129/12	DIS/DEC- 965/55005/11	Przetwarzanie (kodowanie) nr PESEL na karcie miejskiej	oddalenie skargi
32.	18.04.2012 II SA/Wa 2710/11	DOLiS/DEC- 825/11/45756, 45759	Skarga na decyzję GIODO w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji i stwierdzenie, że nie podlega wykonaniu w całości
33.	19.04.2012 II SA/Wa 1885/10	DOLiS/DEC- 1129/10/37954, 37958	Skarga na decyzję w przedmiocie ochrony danych osobowych	zasądzenie od GIODO zwrotu kosztów postępowania
34.	19.04.2012 II SA/Wa 2651/11	GI-DS.-430/614/02	Skarga na niewykonanie przez GIODO wyroku NSA	oddalenie skargi
35.	19.04.2012 II SA/Wa 284/12	GI-DOLiS- 430/254/07	Skarga na niewykonanie przez GIODO wyroku WSA	oddalenie skargi
36.	26.04.2012 II SA/Wa 48/12	DOLiS/DEC- 1009/11/57425, 57427,57429	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi



37.	30.04.2012 II SA/Wa 24/12	DOLiS-440-179/07	Skarga na niewykonanie przez GODO wyroku WSA w Warszawie	oddalenie skargi
38.	30.04.2012 II SA/Wa 108/12	DOLiS-440-83/12	Skarga na bezczynność w przedmiocie przetwarzania danych osobowych	oddalenie skargi
39.	25.05.2012 II SAB/Wa 2/12	DOLiS-440-563/11	Skarga na bezczynność w przedmiocie przetwarzania danych osobowych	oddalenie skargi
40.	29.05.2012 II SA/Wa 188/12	DOLiS/DEC-990/11/56213, 56218,56222	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji i decyzji jej poprzedzającej oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
41.	30.05.2012 II SA/Wa 108/12	DOLiS/DEC-424/10/15798, 15801,15805	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
42.	04.06.2012 II SA/Wa 289/12	DOLiS/DEC-15/12/901,906	Skarga na decyzję w przedmiocie spełnienia obowiązku informacyjnego	uchylenie zaskarżonej decyzji i decyzji jej poprzedzającej oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
43.	06.06.2012 II SA/Wa 453/12	DOLiS/DEC-55/12/3326,3331	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji i decyzji jej poprzedzającej oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
44.	18.06.2012 II SA/Wa 366/12	DOLiS/DEC-31/12/1722,1725	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
45.	19.06.2012 II SA/Wa 166/12	DOLiS/DEC-1082/11/63125, 63129	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
46.	21.06.2012 I OSK 769/12	DOLiS/DEC-585/11/33912	Skarga na decyzję w przedmiocie odmowy udostępnienia informacji publicznej	oddalenie skargi kasacyjnej
47.	22.06.2012 II SA/Wa 629/12	DOLiS/DEC-83/12/6241,6243	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	stwierdzenie nieważności zaskarżonej decyzji oraz decyzji jej poprzedzającej, a także stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
48.	22.06.2012 II SA/Wa 307/12	DOLiS/DEC-707/11/39996, 39992,39995	Skarga na decyzję w przedmiocie usunięcia uchybień w zakresie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji oraz decyzji jej poprzedzającej, a także stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
49.	27.06.2012 II SA/Wa 121/12	DOLiS/POST-252/11/56551	Skarga na postanowienie w przedmiocie oddalenia skargi na bezczynność	uchylenie zaskarżonego postanowienia oraz postanowienia je poprzedzającego, a także stwierdzenie, że zaskarżone postanowienie nie podlega wykonaniu w całości

50.	05.07.2012 II SA/Wa 630/12	DIS/DEC- 103/12/7510	Niewyznaczenie administratora bezpieczeństwa informacji	oddalenie skargi
51.	26.07.2012 II SA/Wa 2672/11	DOLiS/DEC- 822/11/45372, 45373,45374	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	oddalenie skargi
52.	02.08.2012 II SA/Wa 631/12	DIS/DEC- 112/12/7893	Niezgłoszenie do rejestracji zbioru danych zebranych poprzez system monitoringu wizyjnego	zawieszenie postępowania
53.	03.08.2012 II SA/Wa 1242/12	DOLiS-440-559/11	Wniosek o wstrzymanie wykonania decyzji z dnia 26.06.2012 r. oraz poprzedzającej jej decyzji z dnia 23.12.2011 r.	wstrzymanie wykonania decyzji
54.	03.08.2012 II SA/Wa 2733/11	DOLiS/DEC- 924/11/53107, 53108	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
55.	30.08.2012 II SAB/Wa 233/12	bezczytność	Odmowa udostępnienia informacji publicznej	oddalenie skargi
56.	07.09.2012 II SA/Wa 2734/11	DOLiS/DEC- 720/11/40257, 40262	Wniosek o wstrzymanie wykonania decyzji z dnia 24.08.2011 r.	odmowa wstrzymania wykonania decyzji
57.	21.09.2012 I OSK 2016/12	DOLiS/DEC- 20/12/1409,1411, 1413	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	oddalenie skargi kasacyjnej
58.	25.09.2012 II SAB/Wa 34/12	DOLiS-440-443/11	Skarga na przewlekłość postępowania	stwierdzenie, że przewlekłość postępowania nie miała miejsca z rażącym naruszeniem prawa oraz umorzenie postępowania
59.	26.09.2012 I OSK 2074/11	DOLiS/POST- 31/11/6560,6561, 6564	Skarga na postanowienie w przedmiocie zawieszenia postępowania w sprawie przetwarzania danych osobowych	uchylenie zaskarżonej decyzji
60.	26.09.2012 II SA/Wa 428/12	DOLiS/POST- 10/12/2548,2552	Skarga na postanowienie w przedmiocie stwierdzenia uchybienia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy	umorzenie postępowania
61.	26.09.2012 II SA/Wa 649/12	DOLiS/DEC- 64/12/4746,4753	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi
62.	02.10.2012 II SA/Wa 1401/12	DIS/DEC- 649/12/43466	Odmowa udostępnienia informacji publicznej	oddalenie skargi
63.	03.10.2012 II SA/Wa 365/12	DOLiS/DEC- 25/12/1460,1461	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	uchylenie zaskarżonej decyzji oraz decyzji jej poprzedzającej, a także stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
64.	11.10.2012 I OSK 2445/12	DIS/DEC- 103/12/7510	Niewyznaczenie administratora bezpieczeństwa informacji	odmowa wstrzymania wykonania zaskarżonej decyzji
65.	18.10.2012 II SA/Wa 697/12	DOLiS/DEC- 85/12/6240/12, 6242/12	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	oddalenie skargi
66.	22.10.2012 II SA/Wa 1295/12	DOLiS/DEC- 419/12/29747, 29750	Skarga na decyzję w przedmiocie umorzenia postępowania	oddalenie skargi
67.	25.10.2012 II SA/Wa 67/12	DOLiS/DEC- 783/11/43082, 43085,43095	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
68.	09.11.2012 II SA/Wa 124/12	DOLiS/DEC- 943/11/54139,	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	oddalenie skargi

		54141,54146		
69.	13.11.2012 II SAB/Wa 369/12	DOLiS-440-880/11	Skarga na przewlekłe prowadzenie postępowania	umorzenie postępowania
70.	20.11.2012 II SA/Wa 1233/12	DOLiS/DEC-364/12/27317, 27319,27320	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
71.	21.11.2012 I OZ 850/12	DOLiS/DEC-318/12/23575, 13580,23585	Zażalenie GODO na postanowienie WSA w Warszawie o wstrzymaniu wykonania decyzji z dnia 14 sierpnia 2012 r.	oddalenie zażalenia
72.	22.11.2012 I OZ 862/12	DOLiS/DEC-373/12/27562, 27570	Zażalenie GODO na postanowienie WSA w Warszawie o wstrzymaniu wykonania decyzji z dnia 3 sierpnia 2012 r.	oddalenie zażalenia
73.	22.11.2012 II SAB/Wa 400/12	DOLiS-067-37/12	Skarga na bezczynność GODO	oddalenie skargi
74.	28.11.2012 II SAB/Wa 359/12	DOLiS-440-876/11	Skarga na bezczynność GODO	oddalenie skargi
75.	30.11.2012 II SA/Wa 1160/12	DOLiS/DEC-316/12/23561, 23562	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	oddalenie skargi
76.	30.11.2012 II SA/Wa 1137/12	DOLiS/DEC-281/12/21720, 21722,21731	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	oddalenie skargi
77.	03.12.2012 II SA/Wa 1796/12	DOLiS/DEC-727/12/47540, 47542	Wniosek o wstrzymanie wykonania decyzji z dnia 31.07.2012 r.	wstrzymanie wykonania zaskarżonej decyzji
78.	05.12.2012 II SA/Wa 1145/12	DOLiS/DEC-418/12/29729, 29736	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji oraz decyzji jej poprzedzającej, a także stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
79.	13.12.2012 II SA/Wa 1661/12	DOLiS/DEC-586/12/39995, 40001	Skarga na decyzję w przedmiocie ochrony danych osobowych	oddalenie skargi
80.	20.12.2012 II SA/Wa 1567/12	DOLiS/DEC-618/12/42348, 42351,42353	Skarga na decyzję w przedmiocie ochrony danych osobowych	uchylenie zaskarżonej decyzji oraz decyzji jej poprzedzającej, a także stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
81.	27.12.2012 II SA/Wa 2733/11	DOLiS/DEC-924/11/53107, 53108	Wniosek o przywrócenie terminu	oddalenie wniosku

**Informacje przekazane przez organy ścigania  
w sprawach skierowanych w 2012 r.  
przez Generalnego Inspektora Ochrony Danych Osobowych  
zawiadomień o popełnieniu przestępstwa**

<b>Informacja</b>	<b>Rok 2010</b>	<b>Rok 2011</b>	<b>Rok 2012</b>
Umorzenie dochodzenia	11	14	9
Umorzenie dochodzenia w części	-	-	
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	1	-	
Umorzenie dochodzenia i odmowa podjęcia go na nowo	2	1	
Wszczęcie dochodzenia	3	10	
Odmowa wszczęcia dochodzenia	3	3	3
Wszczęcie śledztwa i jego umorzenie	-	-	
Zawieszenie dochodzenia	-	1	
Skierowanie sprawy do sądu	-	1	
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	-	1	1
Brak informacji	-	1	1

## Wykaz szkoleń przeprowadzonych przez GIODO w 2012 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	12.01.2012	Warszawa	Warszawskie Centrum Innowacji Edukacyjnych i Szkoleń
2.	08.02.2012	Warszawa	Ministerstwo Spraw Zagranicznych
3.	13.02.2012	Warszawa	Krajowy Zarząd Gospodarki Wodnej
4.	16.02.2012	Warszawa	Centrum Rozwoju Zasobów Ludzkich
5.	17.02.2012	Warszawa	Doradcy i konsultanci ośrodków doskonalenia nauczycieli z Wrocławia, Skierniewic, Sieradza i Konina oraz dyrektorzy szkół z Gliwic i Częstochowy
6.	23-24.02.2012	Luksemburg	Dyrekcja Tłumaczeń Pisemnych Komisji Europejskiej
7.	27.02.2012	Warszawa	Najwyższa Izba Kontroli
8.	01.03.2012	Warszawa	Centrum Rozwoju Zasobów Ludzkich
9.	05.03.2012	Częstochowa	Urząd Miasta Częstochowa
10.	12.03.2012	Warszawa	Najwyższa Izba Kontroli
11.	20.03.2012	Warszawa	Ministerstwo Nauki i Szkolnictwa Wyższego
12.	20.03.2012	Warszawa	Narodowe Centrum Badań i Rozwoju
13.	21.03.2012	Kielce	Stowarzyszenie „Miasta w Internecie”
14.	26.03.2012	Kraków	Regionalna Wojskowa Pracownia Psychologiczna
15.	28.03.2012	Warszawa	Polska Organizacja Handlu i Dystrybucji
16.	28.03.2012	Warszawa	Centrum Rozwoju Zawodowego Ministerstwa Spraw Zagranicznych
17.	29.03.2012	Warszawa	Agencja Restrukturyzacji i Modernizacji Rolnictwa
18.	12.04.2012	Warszawa	Prokuratura Generalna
19.	17.04.2012	Warszawa	Bank Pocztowy
20.	23.04.2012	Sopot	Spółdzielcza Kasa Oszczędnościowo - Kredytowa
21.	23-24.04.2012	Warszawa	Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych
22.	24.04.2012	Sopot	Urząd Miasta Sopot
23.	09.05.2012	Warszawa	Narodowe Centrum Badań i Rozwoju
24.	09.05.2012	Warszawa	Centrum Rozwoju Zawodowego Ministerstwa Spraw Zagranicznych
25.	09.05.2012	Warszawa	Hays Poland Sp. z o. o.
26.	10.05.2012	Poznań	Uniwersytet Ekonomiczny w Poznaniu
27.	18.05.2012	Warszawa	Bank Pocztowy
28.	21.05.2012	Warszawa	Okręgowa Izba Radców Prawnych
29.	22.05.2012	Warszawa	Narodowy Bank Polski - przedstawiciele banków centralnych państw Europy Wschodniej i Południowo -Wschodniej
30.	22.05.2012	Zalesie Górne	Narodowy Bank Polski

31.	22-23.05.2012	Popowo	Centralny Zarząd Służby Więziennej
32.	28.05.2012	Warszawa	Almamer Szkoła Wyższa - wykład dla studentów i pracowników branży turystycznej
33.	01.06.2012	Wadowice	Centralna Biblioteka Wojskowa w Warszawie - szkolenie dla pracowników bibliotek wojskowych i ośrodków informacji naukowej
34.	04.06.2012	Warszawa	Akademia Obrony Narodowej
35.	05.06.2012	Warszawa	Centrum Rozwoju Zawodowego Ministerstwa Spraw Zagranicznych
36.	12.06.2012	Wrocław	Urząd Miasta Wrocław - szkolenie dla 800 pracowników samorządu terytorialnego
37.	14.06.2012	Kielce	Wojewódzki Urząd Pracy w Kielcach
38.	21.06.2012	Łomża	Sąd Okręgowy w Łomży - szkolenie dla pracowników sądu okręgowego i sądów rejonowych
39.	22.06.2012	Łomża	Sąd Okręgowy w Łomży - szkolenie dla pracowników sądu okręgowego i sądów rejonowych
40.	25.06.2012	Warszawa	Kasa Rolniczego Ubezpieczenia Społecznego - szkolenie dla przedstawicieli KRUS z 16 województw
41.	17.07.2012	Warszawa	Ministerstwo Spraw Zagranicznych
42.	19.07.2012	Warszawa	Szkolenie sektorowe dla przedstawicieli Zarządów Dróg Wojewódzkich
43.	04.09.2012	Warszawa	Służba Wywiadu Wojskowego
44.	07.09.2012	Łysomice	Sąd Okręgowy w Płocku
45.	12.09.2012	Warszawa	Krajowa Rada Sądownictwa
46.	14.09.2012	Smólnik	Sąd Okręgowy we Włocławku
47.	25.09.2012	Wrocław	Urząd Miasta Wrocław, Dolnośląski Urząd Wojewódzki, Urząd Marszałkowski Województwa Dolnośląskiego - szkolenie sektorowe dla przedstawicieli samorządu terytorialnego (ok. 800 uczestników)
48.	27.09.2012	Warszawa	Ośrodek Rozwoju Polskiej Edukacji za Granicą
49.	01.10.2012	Otwock	Ministerstwo Finansów, Departament Wywiadu Skarbowego
50.	02.10.2012	Kraków	Małopolski Instytut Samorządu Terytorialnego - szkolenie sektorowe dla sekretarzy gmin podkarpackich
51.	16.10.2012	Warszawa	Komenda Główna Straży Granicznej - szkolenie sektorowe dotyczące SIS
52.	16.10.2012	Warszawa	Ministerstwo Spraw Zagranicznych
53.	25-26.10.2012	Warszawa	Przedstawiciele szkół i placówek doskonalenia zawodowego nauczycieli w ramach ogólnopolskiego Programu edukacyjnego „Twoje dane - twoja sprawa (...)”
54.	05.11.2012	Warszawa	Kancelaria Sejmu i Kancelaria Senatu
55.	15.11.2012	Warszawa	Kancelaria Sejmu
56.	22.11.2012	Dąbrowa Górnicza	Urząd Miasta w Dąbrowie Górniczej - szkolenie dla przedstawicieli administracji publicznej w ramach I Dnia Otwartego w Dąbrowie Górniczej
57.	24-25.11.2012	Kraków	Okręgowa Rada Adwokacka w Krakowie
58.	27.11.2012	Warszawa	Ministerstwo Spraw Zagranicznych
59.	27.11.2012	Warszawa	Kancelaria Sejmu
60.	29.11.2012	Warszawa	Biuro Rzecznika Praw Obywatelskich
61.	12.12.2012	Warszawa	Ministerstwo Spraw Zagranicznych
62.	13.12.2012	Kielce	Szkolenie sektorowe dla dyrektorów szkół i przedszkoli w ramach ogólnopolskiego Programu edukacyjnego „Twoje dane - twoja sprawa (...)”, zorganizowane przez

			Samorządowy Ośrodek Doradztwa Metodycznego i Doskonalenia Nauczycieli w Kielcach
63.	14.12.2012	Warszawa	Fundacja Rozwoju Społeczeństwa Obywatelskiego
64.	18.12.2012	Warszawa	Kancelaria Sejmu
65.	18.12.2012	Warszawa	Agencja Rynku Rolnego
66.	20.12.2012	Warszawa	Warszawski Uniwersytet Medyczny

**Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych  
w 2012 r.**

1. Akcja „Nie kopiuj głupoty”. Organizator: portal nasza-klasa.pl .
2. II edycja Konkursu „Bezpieczny eSklep 2012”. Organizator: Instytut Logistyki i Magazynowania w Poznaniu.
3. Konferencja „Aktualne problemy dostępu do informacji publicznej”. Organizator: Wydział Prawa i Administracji UKSW oraz Naukowe Centrum Prawno - Informatyczne. Warszawa, 11 stycznia 2012 r.
4. V Konferencji SEMAFOR (Security, Management, Audit, Forum). Organizator: ISACA Warsaw Chapter oraz ISSA Polska. Warszawa, 24-25 lutego 2012 r.
5. 6. Międzynarodowa Konferencja Fundraisingu. Organizator: Polskie Stowarzyszenie Fundraisingu. Warszawa, 09-10 maja 2012 r.
6. Obchody Światowego Dnia Społeczeństwa Informacyjnego w Polsce 2012 oraz Konferencja „Internet w Polsce – dziś i jutro”. Organizator: Polskie Towarzystwo Informatyczne. Warszawa, 17-18 maja 2012 r.
7. Forum IAB „Adaptive Marketing, Adaptive Enterprise”. Organizator: Związek Pracodawców Branży Internetowej IAB Polska, Warszawa, 23-24 maja 2012 r.
8. VIII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Zakopane, 23-25 maja 2012 r.
9. XII Bałtyckie Targi Militarne BALT-MILITARY-EXPO, połączone z V Międzynarodową Konferencją Naukowo-Techniczną „Technologie morskie dla obronności i bezpieczeństwa” NATCON. Organizator: OBR Centrum Techniki Morskiej S.A., Akademia Marynarki Wojennej, Międzynarodowe Targi Gdańskie S.A. Gdańsk, 27-29 czerwca 2012 r.
10. Mazowiecki Konwent Informatyków. Organizator: Redakcja Miesięcznika „IT w Administracji”, 13-14 września 2012 r.
11. XIII Prawnicze Targi Pracy oraz towarzyszące im Prawnicze Targi On – Line. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland. Warszawa, Biblioteka Uniwersytetu Warszawskiego, 9-10 października 2012 r.
12. Konferencja „Cloud Computing – biznes w chmurze”. Organizator: Dziennik Gazeta Prawna. Warszawa, 16 października 2012 r.
13. Konferencja „SECURE 2012”. Organizator: Naukowa i Akademicka Sieć Komputerowa, Warszawa, 22-24 października 2012 r.



14. Wielkopolski Konwent Informatyków. Organizator: Redakcja Miesięcznika „IT w Administracji”, 25-26 października 2012 r.
15. II Konferencja i Narodowy Test Interoperacyjności Podpisu Elektronicznego „CommonSign Warsaw 2012”. Organizator: Instytut Maszyn Matematyczny i Medien Service, Warszawa, 26-27 października 2012 r.
16. Targi Internet Poland oraz Konkursu kreatywnego MIXX-Awards 2012. Organizator: Związek Pracodawców Branży Internetowej IAB Polska, Warszawa, 7-8 listopada 2012 r.
17. Konferencja „Cloud 2012” pod hasłem „Mobilność, wirtualizacja, cloud”. Organizator: Magazyn menedżerów i informatyków „Computerworld”, Warszawa, 8-9 listopada 2012 r.
18. Dolnośląski Konwent Informatyków. Organizator: Redakcja Miesięcznika „IT w Administracji”, 8-9 listopada 2012 r.
19. Konferencja „Monitoring wizyjny – cena za bezpieczeństwo”. Organizator: SecPress.pl. Poznań, 20 listopada 2012 r.
20. „Inside Standard 2012 - 1st Polish-German Bilateral Conference on Standardization - Driver for Security, Privacy and Compliance in Information Systems”. Organizator: Polski Komitet Normalizacji oraz Deutsches Institut für Normung (DIN). Słubice, 21-22 listopada 2012 r.
21. V Konferencja Central European Electronic Card - Warsaw 2012. Payment – Security – Mobility. Organizator: Medien Service. Warszawa, 05-06 grudnia 2012 r.
22. Konferencja „Dokumentacja elektroniczna w podmiotach publicznych”. Organizator: GİODO, Wydział Prawa i Administracji UKSW, Naukowe Centrum Prawno - Informatyczne, Naczelna Dyrekcja Archiwów Państwowych. Warszawa, 06 grudnia 2012 r.
23. Podkarpacki Konwent Informatyków. Organizator: Redakcja Miesięcznika „IT w Administracji”, 13-14 grudnia 2012 r.

**Wykaz konferencji, seminariów i spotkań krajowych i międzynarodowych z udziałem GIODO  
lub jego przedstawicieli, zorganizowanych w 2012 r. w Polsce przez Generalnego Inspektora  
Ochrony Danych Osobowych lub inne podmioty**

<b>L. p.</b>	<b>Data</b>	<b>Konferencja/Seminarium</b>	<b>Miejsce</b>
1.	11.01.2012	Konferencja „Aktualne problemy dostępu do informacji publicznej”. Organizator: Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Naukowe Centrum Prawno-Informatyczne	Warszawa
2.	20.01.2012	Dzień Ochrony Informacji Niejawnych połączony z Dniem Otwartym nt. ochrony informacji. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Wojskowe Zakłady Mechaniczne S.A.	Siemianowice Śląskie
3.	31.01.2012	VI Dzień Ochrony Danych Osobowych. Konferencja „Co Państwo wie o obywatelach? Zasady przetwarzania danych w rejestrach publicznych”. Organizator: GIODO	Warszawa
4.	06.02.2012	Konferencja „Szkola Bezpiecznego Internetu”. Organizator: Fundacja Kidprotect.pl oraz Wyższa Szkoła Nauk Społecznych PEDAGOGIUM w Warszawie	Warszawa
5.	07.02.2012	Dzień Bezpiecznego Internetu. Organizator: Naukowa i Akademicka Sieć Naukowa NASK oraz Fundacja Dzieci Niczyje	Warszawa
6.	08.02.2012	Konferencja „Cloud computing – z biznesem w chmurze”. Organizator: MultiTrain	Warszawa
7.	14.02.2012	Seminarium „Naruszenie prawa w Internecie - jak uzyskać dane sprawcy?”. Organizator: Kancelaria Wierzbowski Eversheds, serwis „IP w Sieci”	Warszawa
8.	16.02.2012	Seminarium eksperckie nt. „Ponowne wykorzystanie informacji sektora publicznego – zagrożenia, wyzwania i szanse dla praw podstawowych.”. Organizator Rzecznik Praw Obywatelskich	Warszawa
9.	23.02.2012	V Konferencja o bezpieczeństwie, audycie i zarządzaniu. Organizator: Computerworld, ISSA Polska oraz ISACA Warsaw Charter	Warszawa
10.	24.02.2012	Warsztaty pt. „Reklama behawioralna”. Organizator: Puls Biznesu	Warszawa
11.	28.02.2012	Seminarium „Nowe Prawo energetyczne i ustawa o odnawialnych źródłach energii” w ramach Kongresu „Trójpak energetyczny. Rynek w nowej rzeczywistości prawnej”. Organizator: Infor Media	Warszawa
12.	01.03.2012	Konferencja „Kształcenie dla e-administracji”. Organizator: Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, Katedra Prawa Informatycznego	Warszawa
13.	06.03.2012	Konferencja „Bezpieczeństwo informacji w nowoczesnej szkole”. Organizator: Śląskie Centrum Społeczeństwa Informacyjnego w Katowicach	Katowice
14.	07.03.2012	I Forum Informatyki Medycznej pt „Elektroniczna informacja medyczna”. Organizator: Centrum Promocji Informatyki	Warszawa
15.	07.03.2012	Konferencja „Reforma regulacji ochrony danych osobowych w Unii Europejskiej. Wstępna ocena jej zakresu i konsekwencji”. Organizator: GIODO, Komisja Europejska, Krajowa Szkoła Administracji Publicznej w Warszawie	Warszawa
16.	08.03.2012	III Forum Bańkowości będącego częścią Polskiego Kongresu Gospodarczego. Organizatorzy: Politechnika Warszawska we współpracy z MM Conferences oraz Stowarzyszeniem	Warszawa

		Emitentów Giełdowych	
17.	09.03.2012	Seminarium „How to litigate before the European Union Courts - seminar for human rights lawyers”. Organizatorzy: Open Society Forum oraz Helsińską Fundację Praw Człowiek	Warszawa
18.	12.03.2012	XII edycja Seminarium w cyklu „Teleinformatyka w przedsiębiorstwach sieciowych” pt. „Uwarunkowania wdrażania smart meteringu. Problemy prawne, technologiczne, społeczne”. Organizator: Centrum Promocji Informatyki	Warszawa
19.	13.04.2012	Spotkanie na Wydziale Bezpieczeństwa Narodowego Akademii Obrony Narodowej w Warszawie	Warszawa
20.	13.03.2012	Konferencja „Przetwarzanie danych osobowych przedsiębiorców”. Organizator: Fundacja Batorego	Warszawa
21.	13.03.2012	Konferencja pt. „Przetwarzanie danych osobowych przedsiębiorców”. Organizator: ENSI i Stowarzyszenie ABI	Warszawa
22.	14.03.2012	II Konferencja „Państwo 2.0. O sprawnym państwie i zarządzaniu z wykorzystaniem IT”. Organizator: Magazyn „Computerworld”	Warszawa
23.	14.03.2012	Spotkanie GIODO z przedsiębiorcami zrzeszonymi w Polskiej Konferencji Pracodawców Prywatnych Lewiatan	Warszawa
24.	15.03.2012	Forum Bankowości Elektronicznej. Organizator: Centrum Promocji Informatyki	Warszawa
25.	20.03.2012	Konferencja „Prawo do prywatności w świecie nowych technologii informatycznych”. Spotkanie GIODO ze studentami i kadrą dydaktyczną Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Organizator: Wydział Prawa, Administracji i Ekonomii UWr	Wrocław
26.	21.03.2012	VII Warsztaty Szkoleniowe „Cyberprzestępczość puka do drzwi administracji – ochrona przeciw włamaniom do sieci urzędowych”. Organizator: Stowarzyszenie „Miasta w Internecie” oraz Świętokrzyskie Partnerstwo dla Rozwoju Społeczeństwa Informacyjnego	Kielce
27.	22.03.2012	VIII Festiwal Nauki w Dąbrowie Górniczej. Organizator: Wyższa Szkoła Biznesu w Dąbrowie Górniczej	Woźniki k/Częstochowy
28.	22.03.2012	VIII Festiwal Nauki w Dąbrowie Górniczej. Organizator: Wyższa Szkoła Biznesu w Dąbrowie Górniczej	Woźniki k/Częstochowy
29.	23.03.2012	Wykład „Dane w rejestrach publicznych jako szczególny rodzaj publicznego zasobu informacyjnego. Własność, jawność, ponowne wykorzystanie” wygłoszony w ramach zebrania naukowego Instytutu Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego w Krakowie	Kraków
30.	29. 03.2012	Konferencja „Poland's Changing Data Protection Law”. Okrągły Stół GIODO ze środowiskiem prawniczym. Organizator: Privacy Law & Business. Data Protection & Privacy Information Worldwide	Warszawa
31.	30.03.2012	Międzynarodowa Konferencja „Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej”. Organizator: Zakład Prawa Administracyjnego Instytutu Nauk Prawnych Polskiej Akademii Nauk w Warszawie	Warszawa
32.	04.04.2012	Warsztaty „Cyfryzacja energetyki w kontekście nowego Prawa Energetycznego - Rozwój Smart Gridu i Smart Meteringu w Polsce”. Organizator: MM Conferences	Warszawa
33.	11.04.2012	Spotkanie z przedstawicielami organizacji pozarządowych nt. opracowania Kodeksu dobrych praktyk. Organizator: GIODO	Warszawa
34.	13.04.2012	Wykład dra Wojciecha. R. Wiewiórowskiego, GIODO, dla studentów studiów doktorskich i kadry naukowo-dydaktycznej Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej.	Warszawa
35.	17.04.2012	Seminarium dla biobanków akademickich i komercyjnych. Organizator: Selvita S.A.	Kraków
36.	18.04.2012	XVIII Forum Informatyki w Administracji pt. „Usługi e-administracji”. Organizator: Centrum Promocji Informatyki	Michałowice k/Warszawy

37.	20-21.04.2012	Ogólnopolskie Seminarium „Prawa i obowiązki stron stosunku pracy – analiza wybranych problemów prawnych”. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland	Warszawa
38.	23-24.04.2012	51. Spotkanie Międzynarodowej Grupy ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska)	Sopot
39.	24.04.2012	2. warsztaty PIAF (Privacy Impact Assessment Framework) dla organów ochrony danych oraz wybranych decydentów politycznych	Sopot
40.	25.04.2012	Debata nt. prawa dla monitoringu wizyjnego. Organizator: Polska Izba Systemów Alarmowych.	Poznań
41.	26.04.2012	VI Europejska Konferencja Dyrektorów Przedszkoli pt. „Kontrola przedszkola kreatywnego”. Organizator: miesięcznik „Dyrektor Szkoły”, kwartalnik „Przed Szkołą. Poradnik dyrektora przedszkola” oraz Wolters Kluwer Polska Sp. z o.o.	Warszawa
42.	27.04.2012	„Spring Biometric Summit 2012”. Organizator: Forum Technologii Bankowych i Związek Banków Polskich	Miedzeszyn k/Warszawy
43.	07.05.2012	Konferencja sekretarzy gmin, miast i powiatów województwa podkarpackiego. Organizator: Małopolski Instytut Samorządu Terytorialnego i Administracji, czyli Krakowski oddział Fundacji Rozwoju Demokracji Lokalnej	Jasionka k/Rzeszowa
44.	09-10.05.2012	6. Międzynarodowa Konferencja Fundraisingu. Organizator: Polskie Stowarzyszenie Fundraisingu.	Warszawa
45.	17.05.2012	II Międzynarodowa Konferencja „Miasto monitorowane – personel, aspekty prawne i technika systemów CCTV”. Organizator: Częstochowska Straż Miejska, Akademia Monitoringu Wizyjnego oraz Krajowa Rada Komendantów Straży Miejskich i Gminnych Rzeczypospolitej Polskiej z siedzibą w Częstochowie	Częstochowa
46.	17-18.05.2012	Konferencja „Internet w Polsce – dziś i jutro” z okazji Światowego Dnia Społeczeństwa Informacyjnego w Polsce 2012. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych	Warszawa
47.	18.05.2012	Seminarium „Bieżące wyzwania polskiego sektora energetycznego. Organizator: Interdyscyplinarne Koło Naukowe Energetyka i Prawo na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego	Warszawa
48.	23.05.2012	XII Forum ADO/ABI. Organizator: Centrum Promocji Informatyki	Warszawa
49.	23-24.05.2012	VI. Forum IAB połączone z targami Internet Poland oraz galą konkursu kreatywnego MIXX-Awards. Organizator: Związek Pracodawców Branży Internetowej IAB Polska	Warszawa
50.	23-25.05.2012	VIII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych	Zakopane
51.	24.05.2012	Seminarium „Skuteczne e-usługi w ubezpieczeniach społecznych”. Organizatorzy: Europejskie Stowarzyszenie ISSA Polska oraz Zakład Ubezpieczeń Społecznych	Warszawa
52.	25.05.2012	Spotkanie GIODO z przedstawicielami biznesu w formule „Śniadania z GIODO”. Organizator: Iron Mountain	Warszawa
53.	28.05.2012	Seminarium „Zagrożenia i wyzwania w procesie przetwarzania danych osobowych w branży hotelarskiej” zorganizowane w ramach cyklu spotkań z serii „Nowe wyzwania edukacji turystycznej”. Organizator: Katedra Gospodarki Turystycznej, Hotelarstwa i Gastronomii Almamer – Szkoła Wyższa	Warszawa
54.	29.05.2012	Konferencja „Cloud computing – przetwarzanie w chmurze”. Organizatorzy: Uniwersytet Kardynała Stefana Wyszyńskiego, Generalny Inspektor Ochrony Danych Osobowych, Szef Agencji Bezpieczeństwa Wewnętrznego oraz Naukowe Centrum Prawno - Informatyczne.	Warszawa
55.	31.05.2012	Konferencja „Innowacyjne technologie i narzędzia pracy prawnika”. Organizator: Wolters Kluwer Polska Sp. z o.o.	Warszawa
56.	01.06.2012	VIII Ogólnopolskie Forum Wojskowych Bibliotek i Ośrodków	Wadowice

		Informacji Naukowej. Organizator: Centralna Biblioteka Wojskowa im. Marszałka Józefa Piłsudskiego	
57.	04-05.06.2012	XII Europejskie Forum Podpisu Elektronicznego pt. „Trust & Security on Digital Single Market”. Organizatorzy: Unizeto Technologies oraz Zachodniopomorski Uniwersytet Technologiczny w Szczecinie	Międzyzdroje
58.	05.06.2012	I Kongres Prawa Bankowego i Informacji zorganizowany w ramach konferencji „Horyzonty Bankowości” z okazji 20-lecia Centrum Prawa Bankowego i Informacji.	Warszawa
59.	13.06.2012	Konferencja z cyklu „Siećspolita” w ramach Forum Debaty Publicznej, na zaproszenie Prezydenta RP	Warszawa
60.	21.06.2012	III Międzynarodowa konferencja Naukowa pt. „Współczesne bezpieczeństwo – wymiar społeczny i jednostkowy”. Organizator: Instytut Nauk Społecznych Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Centralna Biblioteka Wojskowa oraz Siedleckie Towarzystwo Naukowe.	Warszawa
61.	27-29.06.2012	Międzynarodowa Konferencja Naukowo-Techniczna „Technologie morskie dla obronności i bezpieczeństwa” NATKON. Organizator: OBR Centrum Techniki Morskiej S.A., Akademia Marynarki Wojennej, Międzynarodowe Targi Gdańskie S.A.	Gdańsk
62.	11.07.2012	Spotkanie konsultacyjne ze środowiskiem bankowym nt. projektu nowego rozporządzenia Parlamentu Europejskiego i Rady	Warszawa
63.	16-17.08.2012	Konferencja nt. wpływu przetwarzania danych przestrzennych na prywatność osób. Organizator: Katedra Prawa Informatycznego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie oraz Naukowe Centrum Prawno - Informatyczne w Warszawie	Hel
64.	03.09.2012	Spotkanie konsultacyjne ze środowiskiem ubezpieczeniowym nt. unijnej reformy ochrony danych osobowych	Warszawa
65.	05-07.09.2012	VI Powszechny Zjazd Archiwistów Polskich „Zatrzymać przeszłość, dogonić przyszłość”. Organizator: Stowarzyszenie Archiwistów Polskich i Naczelna Dyrekcja Archiwów Państwowych przy współpracy Politechniki Wrocławskiej	Wrocław
66.	10-11.09.2012	Konferencja „Zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów Państwa w obliczu dzisiejszych zagrożeń”. Organizator: Wyższa Szkoła Policji w Szczytnie	Szczytno
67.	13-14.09.2012	Mazowiecki Konwent Informatyków. Organizator: Redakcja Miesięcznika „IT w Administracji”	Grębiszew k/Mińska Mazowieckiego
68.	18.09.2012	Konferencja „Inteligentne sieci – rynek, konsument i zasada zrównoważonego rozwoju”. Organizator: Urząd Regulacji Energetyki	Warszawa
69.	20.09.2012	Konferencja „Nowoczesne technologie w procesie karnym i czynnościach wykrywczych a prawa i wolności obywatelskie. Organizator: Sąd Najwyższy oraz Ministerstwo Sprawiedliwości	Warszawa
70.	24.09.2012	Konferencja specjalistyczna pt. „Prawo, Licencje i Normy we współczesnej szkole”. Organizator: Mazowieckie Kuratorium Oświaty w Warszawie oraz Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie	Warszawa
71.	24-25.09.2012	Kongres Contact Center. Organizator: Nowoczesna Firma S.A.	Warszawa
72.	26.09.2012	II Europejski Kongres Małych i Średnich Przedsiębiorstw. Organizator: Regionalna Izba Gospodarcza w Katowicach, Krajowa Izba Gospodarcza oraz Polska Agencja Rozwoju Przedsiębiorczości	Katowice
73.	27.09.2012	XIII Forum Teleinformatyki „Polska w cyfrowej chmurze”. Organizator: BizTech Consulting	Warszawa
74.	27.09.2012	II Międzynarodowa Konferencja „II Smart Communications & Technology Forum”. Organizator: CBE Polska – Center for Business Education	Gdańsk
75.	28.09.2012	Konferencja Edu Trendy 2012. Organizatorzy: Wolters Kluwer	Warszawa

		Polska, RedNet Media, Dyrektor Szkoły – Miesięcznik Kierowniczej Kadry Oświatowej oraz Przed Szkołą – Poradnik Dyrektora Przedszkola	
76.	28.09.2012	„Budowa kompetencji cyfrowych w administracji publicznej” wykład wprowadzający do „Forum Młodych Mistrzów” podczas XVIII Forum Teleinformatyki „Polska w cyfrowej chmurze?”	Miedzeszyn k/Warszawy
77.	29-30.09.2012	Konferencja „EUROPOL – zwalczanie poważnej i zorganizowanej przestępczości w Europie. Ochrona informacji i danych osobowych”	Koszalin
78.	01.10.2012	II Konferencja bezpieczeństwa ochrony fizycznej i zabezpieczeń technicznych osób, mienia, obiektów i informacji. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych	Spała
79.	05.10.2012	Otwarcie Studiów Podyplomowych w zakresie <i>cloud computingu</i> w Szkole Głównej Handlowej w Warszawie. Wykład inauguracyjny GIODO pt. „Bariery prawne rozwoju nowoczesnych technologii”	Warszawa
80.	08.10.2012	Konferencja „Twoje dane – twoja sprawa. Prawo do prywatności i ochrony danych osobowych we współczesnej szkole”. Organizator: GIODO	Warszawa
81.	12.10.2012	Seminarium nt. monitoringu wizyjnego. Organizator: GIODO, Rzecznik Praw Obywatelskich i Fundacja Panoptykon	Warszawa
82.	16.10.2012	Spotkanie GIODO z przedsiębiorcami. Organizator: Iron Mountain	Warszawa
83.	16.10.2012	Konferencja pt. „Cloud computing – biznes w chmurze”. Organizator: Dziennik Gazeta Prawna	Warszawa
84.	17.10.2012	Seminarium w ramach projektu „Obywatele i wybory”. Organizator: Fundacja im. Stefana Batorego	Warszawa
85.	18.10.2012	XII edycja seminarium „Jakość danych w systemach informatycznych zakładów ubezpieczeń”. Organizator: Polska Izba Ubezpieczeń	Warszawa
86.	19.10.2012	Deбата „Od Administratora do Inspektora”. Organizator: GIODO i Stowarzyszenie Administratorów Bezpieczeństwa Informacji	Warszawa
87.	24.10.2012	Konferencja „Internetowa Publikacja Orzeczeń Sądowych – prawo do sądu i informacji publicznej”. Organizator: Ministerstwo Sprawiedliwości	Warszawa
88.	24.10.2012	VI Forum Komunikacji Publicznej. Organizator: Mennica Polska S.A.	Łódź
89.	24-25.10.2012	Konferencja „Operator Informacji Pomiarowych – nowe narzędzie na rynku energii”. Organizator: Energy Management and Conservation Agency S.A.	Warszawa
90.	25-26.10.2012	II Konferencja i Narodowy Test Interoperacyjności Podpisu Elektronicznego „CommonSign Warsaw 2012”. Organizator: Instytut Maszyn Matematycznych i Medien Service.	Warszawa
91.	29-30.10.2012	Konferencja „Europol – zwalczanie poważnej i zorganizowanej przestępczości w Europie. Ochrona informacji i danych osobowych”. Organizator: Biuro Międzynarodowej Współpracy Policji KGP we współpracy z Komendą Główną Straży Granicznej	Koszalin
92.	08.11.2012	XVI Międzynarodowa Konferencja Energetyczna EUROPOWER. Organizator: MMConferences	Warszawa
93.	08-09.11.2012	Konferencja „Cloud 2012: Mobilność, wirtualizacja, Cloud”. Organizator: Computerworld	Warszawa
94.	05.11.2012	Konferencja „Rozwój elektronicznej administracji w samorządach województwa mazowieckiego wspomagającej niwelowanie dwudzielności potencjału województwa”. Organizator: Marszałek Województwa Mazowieckiego.	Warszawa
95.	13-14.11.2012	Konferencja „10 lat Prawa Nowych Technologii”. Organizator: Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego	Wrocław

96.	21-22.11.2012	Konferencja „Inside Standard 2012 - 1st Polish-German Bilateral Conference on Standardization - Driver for Security, Privacy and Compliance in Information Systems”. Organizator: Polski Komitet Normalizacji i Deutsches Institut für Normung (DIN). Collegium Polonicum.	Słubice
97.	27.11.2012	XXVI Forum Bankowości Elektronicznej – technologie biometryczne w bankowości, rozwój zastosowań, uwarunkowania technologiczne i prawne. Organizator: Centrum Promocji Informatyki	Warszawa
98.	04-06.12.2012	IX Doroczna Konferencja PPBW „Nowe kierunki badań nad bezpieczeństwem wewnętrznym oraz ich praktyczne wykorzystanie”. Organizator: Polska Platforma Bezpieczeństwa Wewnętrznego	Będlewo k/Poznania
99.	05-06.12.2012	V Konferencja Central European Electronic Card - Warsaw 2012. Payment – Security – Mobility. Organizator: Medien Service	Warszawa
100.	06.12.2012	Konferencja naukowa „Dokumentacja elektroniczna w podmiotach publicznych”. Organizator: Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Generalny Inspektor Ochrony Danych Osobowych, Naczelna Dyrekcja Archiwów Państwowych oraz Naukowe Centrum Prawno-Informatyczne.	Warszawa
101.	06.12.2012	Kongres Akademickich Biur Karier. Organizator: Uniwersytet Warszawski, Rzecznik Praw Absolwenta, Ministerstwo Nauki i Szkolnictwa Wyższego	Warszawa
102.	12.12.2012	Spotkanie z Panem Giovannim Buttarellim, Zastępcą Europejskiego Rzecznika Ochrony Danych Osobowych. Organizator: GODO	Warszawa
103.	13.12.2012	X Konferencja naukowa „Biometria 2012”. Organizator: Instytut Maszyn Matematycznych	Warszawa

**Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem  
GODO lub jego przedstawicieli, które odbyły się w 2012 r. za granicą**

<b>L. p.</b>	<b>Data</b>	<b>Konferencja/Seminarium/Spotkanie</b>	<b>Miejsce</b>
1.	10-12.01.2012	Posiedzenie Podgrupy ds. BCR	Bruksela
2.	11-12.01.2012	Posiedzenie Podgrupy ds. Technologii	Bruksela
3.	18-19.01.2012	Spotkanie w Komisji Europejskiej w sprawie Obchodów VI Europejskiego Dnia Ochrony Danych Osobowych	Bruksela
4.	23-24.01.2012	II symposium Europejskiej Sieci Tematycznej „Legal Aspects of Public Sector Information” (LAPSI) zorganizowane w University Foundation w Brukseli.	Bruksela
5.	24.01.2012	Spotkanie GODO z polskimi europosłami w Brukseli nt. reformy ochrony prywatności z okazji obchodów VI Europejskiego Dnia Ochrony Danych Osobowych	Bruksela
6.	25-27.01.2012	Międzynarodowa Konferencja z okazji obchodów VI Europejskiego Dnia Ochrony Danych Osobowych pt. „Computers, Privacy and Data Protection (CPDP) 2012. European Data Protection: Coming Of Age”. Organizator: Vrije Universiteit Brussel (Research Group on Law, Science, Technology and Society LSTS), Facultés Universitaires de Namur (Centre de Recherches Informatique et Droit CRID), Institut National de Recherche en Informatique et en Automatique INRIA, Tilburg University (Tilburg Institute for Law, Technology, and Society TILT) oraz Fraunhofer Institut für System- und Innovationsforschung ISI	Bruksela
7.	01-02.02.2012	84. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych	Bruksela
8.	05-07.02.2012	Spotkanie w sprawie ewaluacji Schengen. Organizator: czeski Organ Ochrony Danych Osobowych	Praga
9.	08-10.02.2012	Spotkanie w sprawie ewaluacji Schengen. Organizator: słowacki Organ Ochrony Danych Osobowych	Bratysława
10.	09-11.02.2012	Posiedzenie Wspólnych Organów Nadzorczych	Lizbona
11.	16.02.2012	Seminarium Rady Europy „Ochrona danych osobowych i media”. Organizator: Dyrekcja Generalna ds. Praw Człowieka i Spraw Prawnych	Kijów
12.	20-22.02.2012	Spotkanie nt. „Ochrony danych osobowych: mechanizmy zadośćuczynienia i ich wykorzystanie”. Organizator: Europejska Agencja Praw Podstawowych	Wiedeń
13.	20-24.02.2012	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy oraz Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
14.	28-29.02.2012	Spotkanie Podgrupy ds. Technologii	Bruksela
15.	05-06.03.2012	Posiedzenie Podgrupy ds. Biometrii Grupy Roboczej Art. 29	Bruksela
16.	05-06.03.2012	2. Spotkanie europejskiego wielostronnego Forum ds. Elektronicznego Fakturowania	Bruksela
17.	12.03.2012	Spotkanie dotyczące misji ewaluacyjnej Schengen w Słowacji	Bruksela
18.	13-15.03.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
19.	14-16.03.2012	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
20.	22-23.03.2012	85. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych	Bruksela
21.	10.04.2012	Seminarium „Jak postępować z danymi osobowymi: rekomendacje dla mediów”. Organizator: Dyrekcja Generalna ds. Praw Człowieka i Spraw Prawnych	Kijów
22.	15-17.04.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and	Bruksela



		Data Protection – DAPIX)	
23.	19-21.04.2012	Konferencja „Rewizja przepisów dyrektywy o ochronie danych UE”. Organizator: Centre for European Legal Studies (CELS)	Cambridge
24.	03-04.05.2012	Wiosenna Konferencja Rzeczników Ochrony Danych 2012 „Sprostać oczekiwaniom? Nowe ramy prawne ochrony danych Unii Europejskiej”. Organizator: Luksemburski Organ Ochrony Danych Osobowych	Luksemburg
25.	07.05.2012	Międzynarodowa Konferencja „2. Europejski Dzień Ochrony Danych EDPD 2012. Reforma europejskiego prawa ochrony danych”. Organizator: EUROFORUM Deutschland	Berlin
26.	08.05.2012	Posiedzenie Podgrupy Roboczej ds. BCR	Bruksela
27.	09-10.05.2012	Warsztaty Komisji Europejskiej poświęcone dostępowi do orzeczeń sądowych, prawie do anonimowości i ochronie danych osobowych, współorganizowane przez Macedońską Agencję Ochrony Danych	Skopje
28.	10.05.2012	3. Coroczne Sympozjum Agencji Praw Podstawowych UE pt. "The EU Data Protection Reform: New Fundamental Rights Guarantees"	Wiedeń
29.	11.05.2012	Posiedzenie Podgrupy ds. Kluczowych Postanowień Dyrektywy Dyrektywy (Key Provisions)	Bruksela
30.	13-15.05.2012	Międzynarodowe Spotkanie Grupy utworzonej w Mexico City dt. egzekwowania prawa „Réunion internationale sur l'application de la loi". Organizator: Kanadyjski Rzecznik Ochrony Prywatności	Montreal
31.	14-15.05.2012	Warsztaty Komisji Europejskiej dotyczące ochronie prywatności konsumentów w Internecie, współorganizowane przez Macedońską Agencję Ochrony Danych	Skopje
32.	14-15.05.2012	Spotkanie Podgrupy ds. Technologii	Bruksela
33.	21.05.2012	Międzynarodowa Konferencja „Personal Data Protection: Legislation, Practices, Enforcement". Organizatorzy: Centrum Badawcze Informatyki Prawniczej Ukraińskiej Akademii Nauk Prawnych, Instytut Zasobów Informacyjnych Ukraińskiej Akademii Nauk oraz czasopismo „Business and Security"	Kijów
34.	21-22.05.2012	14. Spotkanie Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA)	Kijów
35.	22-23.05.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
36.	22-24.05.2012	Posiedzenie Grupy Roboczej EURODAC, Podgrupy Roboczej ds. Granic, Podróży i Egzekwowania Prawa (BTLE) oraz Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions)	Bruksela
37.	30-31.05.2012	Międzynarodowa Konferencja „Modernizacja przepisów o ochronie danych w Europie”. Organizator: Dyrektoriat Ochrony Danych Osobowych Macedonii	Skopje
38.	04.06.2012	Dyskusja ekspercka poświęcona ochronie prywatności w kontekście relacjonowania przez media wyborów parlamentarnych na Ukrainie. Organizator: Rada Europy	Kijów
39.	06-07.06.2012	86. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych	Bruksela
40.	13-14.06.2012	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
41.	19-22.06.2012	28. Posiedzenie Plenarne Komitetu Konsultacyjnego ds. Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD)	Strasburg
42.	27.06.2012	Konferencja Komisji Europejskiej dotycząca przyszłości projektu e-Justice.	Bruksela
43.	28.06.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela
44.	02-04.07.2012	25. Doroczna Międzynarodowa Konferencja Privacy Laws & Business „Pokonywanie przeszkód w ochronie prywatności”	Cambridge
45.	03-04.07.2012	Seminarium Rady Europy dotyczące ochrony danych osobowych w działalności mediów	Kijów
46.	10.07.2012	Posiedzenie Podgrupy Roboczej ds. BCR	Bruksela

47.	11-12.07.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
48.	02-04.09.2012	24. warsztaty rozpatrywania spraw zorganizowane przez węgierski organ ochrony danych	Budapeszt
49.	03-04.09.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela
50.	04.09.2012	Posiedzenie Podgrupy ds. Biometrii & eGovernment Grupy Roboczej Art. 29	Bruksela
51.	06.09.2012	Spotkanie Podgrupy ds. Technologii	Bruksela
52.	07.09.2012	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
53.	09-11.09.2012	52. Spotkanie Międzynarodowej Grupy ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska)	Berlin
54.	13.09.2012	Spotkanie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions) Grupy Roboczej Art. 29	Bruksela
55.	18.09.2012	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
56.	25-26.09.2012	87. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych	Bruksela
57.	26.09.2012	2. Spotkanie Europejskiego Forum ds. e-fakturowania	Bruksela
58.	26-27.09.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela
59.	27.09.2012	3. Konferencja PIAF (Privacy Impact Assessment Framework)	Bruksela
60.	30.09-1.10.2012	Seminarium Rady Europy dotyczące ochrony danych osobowych	Kijów
61.	03.10.2012	Warsztat pt. „Ochrona danych w badaniach farmaceutycznych i bezpieczeństwo leków: dialog między organami ochrony danych i sektorem farmaceutycznym”. Organizator: International Pharmaceutical Privacy Consortium w Paryżu	Paryż
62.	03-04.10.2012	Posiedzenie Wspólnego Organu Nadzorczego ds. Schengen i Wspólnego Organu Nadzorczego nad Europolem	Bruksela
63.	04.10.2012	Posiedzenie Wspólnego Organu Nadzorczego ds. Celnych	Bruksela
64.	09-10.10.2012	Międzyparlamentarne Posiedzenie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych pt. „Reforma ram prawnych UE w zakresie ochrony danych – budowanie zaufania w cyfrowym, zglobalizowanym świecie”. Organizator: Komisja LIBRE-PE	Bruksela
65.	15-16.10.2012	Spotkanie Podgrupy ds. Technologii	Ateny
66.	22-26.10.2012	34. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności. Organizator: Jednostka ds. Regulacji i Kontroli Danych Osobowych (URCDP)	Punta del Ester
67.	09.11.2012	Seminarium dla pracowników albańskiego urzędu rzecznika ochrony danych osobowych.	Tirana
68.	11-25.11.2012	Wymiana pracowników w ramach projektu mobilności LdV	Sofia
69.	12-13.11.2012	Spotkanie Podgrupy ds. Technologii	Bruksela
70.	13.11.2012	Warsztat „Global Interoperability: A Goal within Reach?” w ramach spotkania IAPP (The International Association of Privacy Professionals)	Bruksela
71.	19.11.2012	Posiedzenie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions)	Bruksela
72.	21-22.11.2012	III Międzynarodowa Konferencja „Ochrona Danych Osobowych”. Organizator: Federalna Służba Nadzoru w sektorze Łączności, Technologii Informacyjnych i Masowej Komunikacji Federacji Rosyjskiej.	Moskwa
73.	23.11.2012	Spotkanie Grupy Koordynującej nadzór nad VIS oraz Spotkanie Grupy Koordynującej nadzór nad EURODAC	Bruksela
74.	27-30.11.2012	29. Posiedzenie Plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD)	Strasburg
75.	02-23.12.2012	Wymiana pracowników Biura GłODO w ramach projektu mobilności LdV	Strasburg

76.	03.12.2012	Warsztaty poświęcone ocenie odpowiedniego poziomu ochrony danych osobowych przy przekazywaniu danych do państw trzecich. Organizator: Komisja Europejska w ramach TAIEX.	Skopje
77.	04-06.12.2012	88. posiedzenie Grupy Roboczej Art. 29	Bruksela
78.	10-11.12.2012	Spotkanie Grupy Roboczej ds. Europolu, ds. Eurodac, ds. BTLE	Bruksela

**Wykaz decyzji i postanowień Generalnego Inspektora Ochrony Danych Osobowych  
wydanych w 2012 roku w sprawach o wyrażenie zgody  
na przekazanie danych osobowych za granicę**

<b>Lp.</b>	<b>Data wydania decyzji/ postanowienia</b>	<b>Nazwa podmiotu</b>	<b>Sygnatura decyzji/postanowienia</b>
1.	05.04.2012	Kidde Polska Sp. z o.o., Ropczyce	DESiWM-DEC-285/22452/12 (decyzja wyrażająca zgodę na przekazanie danych)
2.	05.04.2012	Lowe GGK Sp. z o.o., Warszawa	DESiWM/DEC-286/22469/12 (decyzja wyrażająca zgodę na przekazanie danych)
3.	05.04.2012	Novo Nordisk Pharma Sp. z o.o.	DESiWM/DEC-284/22438/12 (decyzja wyrażająca zgodę na przekazanie danych)
4.	05.04.2012	Open and Partners Sp. z o.o., Warszawa	DESiWM/DEC-287/22483/12 (decyzja wyrażająca zgodę na przekazanie danych)
5.	05.04.2012	Pan Media Western Sp. z o.o., Warszawa	DESiWM/DEC-288/22510/12 (decyzja wyrażająca zgodę na przekazanie danych)
6.	05.04.2012	St. Jude Medical Sp. z o.o.	DESiWM/DEC-282/22427/12 (decyzja wyrażająca zgodę na przekazanie danych)
7.	05.04.2012	St. Jude Medical Sp. z o.o.	DESiWM/DEC-283/22429/12 (decyzja wyrażająca zgodę na przekazanie danych)
8.	17.04.2012	Draftfc + Ad Fabrika Sp. z o.o., Warszawa	DESiWM/DEC-328/24559/12 (decyzja wyrażająca zgodę na przekazanie danych)
9.	17.04.2012	Kompania Piwowarska S.A.	DESiWM/DEC-327/24545/12 (decyzja wyrażająca zgodę na przekazanie danych)
10.	09.05.2012	Charits Europe S.A. Oddział w Polsce Warszawa	DESiWM/DEC-394/28728/12 (decyzja wyrażająca zgodę na przekazanie danych)
11.	20.04.2012	Draftfc + Ad Fabrika Sp. z o.o., Warszawa	DESiWM/POST-105/25766/12 (postanowienie o sprostowaniu oczywistej omyłki pisarskiej)
12.	20.04.2012	Pan Media Western Sp. z o.o., Warszawa	DESiWM/POST-104/25758/12 (postanowienie o sprostowaniu oczywistej omyłki pisarskiej)
13.	20.04.2012	Open and Partners Sp. z o.o., Warszawa	DESiWM/POST-103/25749/12 (postanowienie o sprostowaniu oczywistej omyłki pisarskiej)
14.	20.04.2012	Lowe GGK Sp. z o.o., Warszawa	DESiWM/POST-102/25744/12 (postanowienie o sprostowaniu oczywistej omyłki pisarskiej)
15.	17.07.2012	SEB Leasing Polska Sp. z o.o.	DESiWM/DEC-653/ 43705/12 (decyzja wyrażająca zgodę na przekazanie danych)
16.	17.07.2012	Skandinaviska Enskilda Banken AB S.A., Oddział w Polsce	DESiWM/DEC-654/ 43710/12 (decyzja wyrażająca zgodę na przekazanie danych)
17.	17.07.2012	SEB Commercial Finance Sp. z o.o.	DESiWM/DEC-655/ 43713/12 (decyzja wyrażająca zgodę na przekazanie danych)

			danych)
18.	18.07.2012	UCB Pharma Sp. z o.o.	DESiWM/DEC-673/44419/12 (decyzja wyrażająca zgodę na przekazanie danych)
19.	18.07.2012	Lycamobile Sp. z o.o.	DESiWM/DEC-674/44438/12 (decyzja wyrażająca zgodę na przekazanie danych)
20.	20.09.2012	Dendro Poland LTD Sp. z o.o., Poznań	DESiWM/DEC-894/57036/12 (decyzja o umorzeniu na skutek wycofania wniosku)
21.	04.10.2012	Honda Logistics Center Central Europe Sp. z o.o., Pniewy	DESiWM/DEC-945/60097/12 (decyzja wyrażająca zgodę na przekazanie danych)
22.	04.10.2012	IICS/Polska Sp. z o.o., Warszawa	DESiWM/DEC-944/60094/12 (decyzja wyrażająca zgodę na przekazanie danych)
23.	04.10.2012	Honda Logistics Center Central Europe Sp. z o.o., Pniewy	DESiWM/DEC-946/60159/12 (decyzja wyrażająca zgodę na przekazanie danych)
24.	04.10.2012	AstraZeneca Pharma Poland Sp. z o.o.	DESiWM/DEC-947/60163/12 (decyzja wyrażająca zgodę na przekazanie danych)
25.	16.10.2012	Skandia Życie Towarzystwo Ubezpieczeń S.A., Warszawa	DESiWM/DEC-1008/63267/12 (decyzja wyrażająca zgodę na przekazanie danych)
26.	31.10.2012	Emerson Process Management Power and Water Solutions, Warszawa	DESiWM/DEC-1067/66883/12 (decyzja częściowo umarzająca postępowanie w zakresie przekazania danych do Szwajcarii, w pozostałym zakresie zgoda na przekazanie danych)
27.	31.10.2012	Emerson Process Management Sp. z o.o., Warszawa	DESiWM/DEC-1068/66885/12 (decyzja częściowo umarzająca postępowanie w zakresie przekazania danych do Szwajcarii, w pozostałym zakresie zgoda na przekazanie danych)
28.	19.11.2012	AFH Poland Sp. z o.o., Warszawa	DESiWM/DEC-1155/70235/12 (decyzja o częściowej odmowie wyrażenia zgody na przekazanie danych, w pozostałym zakresie wyrażająca zgodę na przekazanie danych)
29.	03.12.2012	Diversey Poland Services Sp. z o.o., Warszawa	DESiWM/DEC-1217/74455/12 (decyzja wyrażająca zgodę na przekazanie danych)
30.	03.12.2012	Sealed Air Polska Sp. z o.o., Ożarów Mazowiecki	DESiWM/DEC-1218/74459/12 (decyzja wyrażająca zgodę na przekazanie danych)
31.	03.12.2012	Diversey Poland Sp. z o.o., Warszawa	DESiWM/DEC-1219/74461/12 (decyzja wyrażająca zgodę na przekazanie danych)
32.	10.12.2012	Novo Nordisk Pharmaceutical Services Sp. z o.o., Warszawa	DESiWM/DEC-1221/74595/12 (decyzja o umorzeniu na skutek wycofania wniosku)
33.	10.12.2012	Novo Nordisk Pharma Sp. z o.o., Warszawa	DESiWM/DEC-1220/12/74593/ 12 (decyzja o umorzeniu na skutek wycofania wniosku)
34.	10.12. 2012	Amgen Sp. z o.o., Warszawa	DESiWM/DEC-1222/74597/12 (decyzja wyrażająca zgodę na przekazanie danych)
35.	10.12.2012	Amgen Biotechnologia Sp. z o.o.	DESiWM/DEC-1223/74600/12 (decyzja wyrażająca zgodę na przekazanie danych)
36.	27.12.2012	First Data Poland Holding S.A.,	DESiWM-DEC-1272/78196/12

		Warszawa	(decyzja wyrażająca zgodę na przekazanie danych)
37.	27.12.2012	First Data Polska S.A., Warszawa	DESiWM/DEC-1273/78191/12 (decyzja wyrażająca zgodę na przekazanie danych)
38.	27.12.2012	APCE Sp. z o.o.	DESiWM/DEC-1271/78304/12 (decyzja wyrażająca zgodę na przekazanie danych)
39.	27.12.2012	Hyatt International	DESiWM/DEC-1274/78182/12 (decyzja wyrażająca zgodę na przekazanie danych)
40.	28.12.2012	Hewlett-Packard Polska Sp. z o.o., Warszawa	DESiWM/DEC-1276/78213/12 (decyzja wyrażająca zgodę na przekazanie danych)
41.	28.12.2012	Global E-Business Operations Sp. z o.o., Wrocław	DESiWM/DEC-1275/48200/12 (decyzja wyrażająca zgodę na przekazanie danych)
42.	28.12.2012	BP Polska Services Sp. z o.o.	DESiWM/DEC -1282/12/78298/12 (decyzja wyrażająca zgodę na przekazanie danych)
43.	28.12.2012	BP Europe SE, Oddział w Polsce	DESiWM/DEC-1281/78303/12 (decyzja wyrażająca zgodę na przekazanie danych)
44.	31.12.2012	GSK Commercial Sp. z o.o., Warszawa	DESiWM/DEC-1286/78465/12 (decyzja wyrażająca zgodę na przekazanie danych)
45.	31.12.2012	GSK Services Sp. z o.o., Poznań	DESiWM/DEC-1287/78466/12 (decyzja wyrażająca zgodę na przekazanie danych)
46.	31.12.2012	GSK Services Sp. z o.o., Poznań	DESiWM/DEC-1288/78467/12 (decyzja wyrażająca zgodę na przekazanie danych)
47.	31.12.2012	GSK Services Sp. z o.o., Poznań	DESiWM/DEC-1289/78468/12 (decyzja wyrażająca zgodę na przekazanie danych)
48.	31.12.2012	GSK Commercial Sp. z o.o., Warszawa	DESiWM/DEC-1290/78469/12 (decyzja wyrażająca zgodę na przekazanie danych)
49.	31.12.2012	GSK Commercial Sp. z o.o., Warszawa	DESiWM/DEC-1291/78472/12 (decyzja wyrażająca zgodę na przekazanie danych)
50.	31.12.2012	GSK Commercial Sp. z o.o., Warszawa	DESiWM/DEC-1292/78478/12 (decyzja wyrażająca zgodę na przekazanie danych)
51.	31.12.2012	GSK Services Sp. z o.o., Poznań	DESiWM/DEC-1293/78485/12 (decyzja wyrażająca zgodę na przekazanie danych)
52.	31.12.2012	GSK Services Sp. z o.o., Poznań	DESiWM/DEC-1294/78491/12 (decyzja wyrażająca zgodę na przekazanie danych)
53.	31.12.2012	GSK Commercial Sp. z o.o.	DESiWM/DEC-1295/78497/12 (decyzja wyrażająca zgodę na przekazanie danych)
54.	31.12.2012	GSK Services Sp. z o.o., Poznań	DESiWM/DEC-1296/78499/12 (decyzja wyrażająca zgodę na przekazanie danych)
55.	31.12.2012	GSK Commercial Sp. z o.o., Warszawa	DESiWM/DEC-1297/78501/12 (decyzja wyrażająca zgodę na przekazanie danych)