Generalny Inspektor
Ochrony Danych Osobowych

SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2013

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

[1] Niniejsze *Sprawozdanie* obejmuje okres działalności Generalnego Inspektora Ochrony Danych Osobowych od 1 stycznia 2013 r. do 31 grudnia 2013 r.

SPIS TREŚCI

SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W 2013 ROKU

Wprowadzenie

Podstawowym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych, jest Konwencja Nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[2]. Konwencja nałożyła na kraje członkowskie zobowiązanie stworzenia ustawodawstwa w zakresie ochrony danych osobowych, wskazując jednocześnie, w jakim kierunku ustawodawstwo to powinno zmierzać.

Ochrona danych osobowych jest prawem podstawowym, ustanowionym w art. 8 Karty praw podstawowych Unii Europejskiej i w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). 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.

[2] Konwencja Nr 108 RE weszła w życie 1 października 1985 r. Polska ratyfikowała Konwencję w dniu 24 kwietnia 2002 r.

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 GIODO jest uprawniony do:

1. kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
2. wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych,
3. 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.),
4. prowadzenia rejestru zbiorów danych oraz udzielania informacji o zarejestrowanych zbiorach,
5. opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
6. inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
7. 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, rozpowszechnianie informacji z zakresu ochrony danych osobowych oraz współpracę międzynarodową. 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 europejskimi i pozaeuropejskimi organami ochrony danych osobowych oraz instytucjami zajmującymi się szeroko rozumianymi prawami człowieka.

Podstawę prawną działania Generalnego Inspektora Ochrony Danych Osobowych 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:

a) 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)

b) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wraz załącznikiem zawierającym opis środków bezpieczeństwa na poziomie podstawowym, podwyższonym i wysokim (Dz. U. Nr 100, poz. 1024), wydane na podstawie art. 39a ustawy. Rozporządzenie określa:

- sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
- podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
- wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

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

d) 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.

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.

Od 22 marca 2013 r. zaczęły obowiązywać nowe przepisy prawa mające istotny wpływ na ochronę danych osobowych. W tym dniu weszła w życie ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. 2012, poz. 1445), która na dostawcę usług telekomunikacyjnych nakłada obowiązek zawiadamiania GIODO i abonentów o naruszeniu danych osobowych i prowadzenia rejestru takich zdarzeń. Na jej mocy do Prawa telekomunikacyjnego dodano art. 174a-174d, które stanowią że:

1. dostawca publicznie dostępnych usług telekomunikacyjnych **zawiadamia** Generalnego Inspektora Ochrony Danych Osobowych o naruszeniu danych osobowych niezwłocznie, nie później niż w terminie 3 dni od stwierdzenia naruszenia (art. 174a ust. 1);
2. przez naruszenie danych osobowych rozumie się przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych (art. 174a ust. 2);
3. w przypadku, gdy naruszenie danych osobowych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, dostawca publicznie dostępnych usług telekomunikacyjnych niezwłocznie, nie później niż w terminie 3 dni od stwierdzenia naruszenia, zawiadamia o takim naruszeniu również abonenta lub użytkownika końcowego (art. 174a ust. 3);
4. przez naruszenie danych osobowych, które może wywrzeć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, rozumie się takie naruszenie, które w szczególności może skutkować nieuprawnionym posługiwaniem się danymi osobowymi, szkodą majątkową, naruszeniem dóbr osobistych, ujawnieniem

tajemnicy bankowej lub innej ustawowo chronionej tajemnicy zawodowej (art. 174a ust. 4);

5. **zarówno zawiadomienie GIODO**, jak i **zawiadomienie abonenta lub użytkownika końcowego będącego osobą fizyczną** powinny zawierać m.in.: opis charakteru naruszenia danych osobowych, dane kontaktowe dostawcy publicznie dostępnych usług telekomunikacyjnych, informacje o zalecanych środkach mających na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia oraz o działaniach podjętych przez dostawcę, opis skutków naruszenia oraz proponowanych przez dostawcę środków naprawczych. Przy czym zawiadomienie GIODO powinno dodatkowo zawierać informacje o zakładanym ryzyku związanym z powstałym naruszeniem oraz o fakcie (lub jego braku) poinformowania abonenta lub użytkownika końcowego, będącego osobą fizyczną o wystąpieniu naruszenia danych osobowych (art. 174a ust. 7, art. 174a ust. 8);
6. **zawiadomienia GIODO można dokonać na formularzu, który jest dostępny na stronie internetowej www.giodo.gov.pl w zakładce Elektroniczna Skrzynka Podawcza, jak również na stronie internetowej www.epuap.gov.pl;**
7. dostawca publicznie dostępnych usług telekomunikacyjnych nie musi zawiadamiać abonenta lub użytkownika końcowego o naruszeniu, jeżeli wdrożył przewidziane przepisami o ochronie danych osobowych odpowiednie techniczne i organizacyjne środki ochrony, które uniemożliwiają odczytanie danych przez osoby nieuprawnione oraz zastosował je do danych, których ochrona została naruszona (art. 174a ust. 5);
8. jeżeli dostawca publicznie dostępnych usług telekomunikacyjnych nie zawiadomił abonenta lub użytkownika końcowego będącego osobą fizyczną o fakcie naruszenia danych osobowych, **Generalny Inspektor Ochrony Danych Osobowych może nałożyć, w drodze decyzji, na dostawcę obowiązek przekazania abonentom lub użytkownikom końcowym, będącym osobami fizycznymi takiego zawiadomienia**, biorąc pod uwagę możliwe niekorzystne skutki naruszenia (art. 174a ust. 6);
9. dostawca publicznie dostępnych usług telekomunikacyjnych prowadzi **rejestr naruszeń danych osobowych,** w tym faktów towarzyszących naruszeniom, ich skutków i podjętych działań, o których mowa w art. 174a ust. 8 pkt 4 i 6, zawierający w szczególności: opis charakteru naruszenia danych osobowych, informacje o zaleconych przez dostawcę publicznie dostępnych usług telekomunikacyjnych środkach mających na celu złagodzenie ewentualnych niekorzystnych skutków

naruszenia danych osobowych, informacje o działaniach podjętych przez dostawcę publicznie dostępnych usług telekomunikacyjnych, informacje o fakcie poinformowania lub braku poinformowania abonenta lub użytkownika końcowego będącego osobą fizyczną o wystąpieniu naruszenia danych osobowych, opis skutków naruszenia danych osobowych, opis zaproponowanych przez dostawcę publicznie dostępnych usług telekomunikacyjnych środków naprawczych (art. 174d ust. 1);

10. dostawca publicznie dostępnych usług telekomunikacyjnych może powierzyć w drodze umowy, innemu przedsiębiorcy prowadzenie rejestru naruszeń danych osobowych (art. 174d ust. 2);
11. do sprawowanej przez Generalnego Inspektora Ochrony Danych Osobowych kontroli wykonywania przez dostawców publicznie dostępnych usług telekomunikacyjnych wskazanych wyżej obowiązków, stosuje się odpowiednio przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (art. 174b);
12. Generalny Inspektor Ochrony Danych Osobowych, przy kierowaniu do dostawcy publicznie dostępnych usług telekomunikacyjnych wystąpień w trybie art. 19a ustawy o ochronie danych osobowych, uwzględnia wytyczne Komisji Europejskiej dotyczące realizacji obowiązku powiadamiania abonenta lub użytkownika końcowego będącego osobą fizyczną o naruszeniu jego danych osobowych i wskazuje okoliczności, formę i sposób takiego powiadomienia. Generalny Inspektor Ochrony Danych Osobowych może publikować takie wystąpienia na swojej stronie podmiotowej BIP, o ile nie będą one zawierać informacji stanowiących tajemnicę przedsiębiorstwa (art. 174c).

Wprowadzenie ww. przepisów ustawy Prawo telekomunikacyjne było konsekwencją działań legislacyjnych podjętych na szczeblu europejskim, których priorytetem było stworzenie mechanizmów ochronnych oraz zapewnienie bezpieczeństwa osobom korzystającym z usług telekomunikacyjnych. Podjęta została próba usunięcia istotnej bariery hamującej wzrost usług sektora telekomunikacyjnego, jaką jest obawa naruszenia prywatności oraz danych osobowych, w tym danych wrażliwych. Efektem tych działań była nowelizacja dyrektywy 2002/58/WE o prywatności i łączności elektronicznej. Podczas prac nad tekstem dyrektywy pojawiła się wątpliwość, czy w przepisach dotyczących telekomunikacji powinny znaleźć się regulacje odnoszące się do ochrony danych osobowych. Ostatecznie zdecydowano się na częściowe uregulowanie tych kwestii również w unijnym pakiecie

telekomunikacyjnym, co znalazło odzwierciedlenie w ww. art. 174a-174d polskiej znowelizowanej ustawy Prawo telekomunikacyjne.

Artykuł 174 a ustawy Prawo telekomunikacyjne implementuje art. 2 lit. i oraz art. 4 ust. 1 akapit 1 znowelizowanej dyrektywy o prywatności i łączności elektronicznej. Generalny Inspektor Ochrony Danych Osobowych w znowelizowanych przepisach został uznany za organ, któremu dostawcy publicznie dostępnych usług telekomunikacyjnych są obowiązani przesyłać zawiadomienia dotyczące przypadków naruszenia danych osobowych abonentów lub użytkowników końcowych będących osobami fizycznymi. Jeżeli przedsiębiorca nie wywiąże się z tego obowiązku, GIODO będzie mógł podjąć interwencję w tej sprawie, kierując do podmiotu obowiązanego stosowne wystąpienie na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych.

Z kolei przepis art. 174a ust. 5 ustawy Prawo telekomunikacyjne stanowi implementację art. 4 ust. 3 zdanie 3 znowelizowanej dyrektywy, zgodnie z którym powiadomienie danego abonenta lub osoby fizycznej o naruszeniu danych osobowych nie jest wymagane, jeżeli dostawca wykazał – zgodnie z wymogami właściwego organu – że wdrożył odpowiednie technologiczne środki ochrony, oraz że zostały one zastosowane do tych danych, których dotyczyło naruszenie bezpieczeństwa. Tego rodzaju technologiczne środki ochrony muszą sprawiać, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich. Jednocześnie w art. 174a wprowadzona została definicja naruszenia danych osobowych (ust. 2) oraz naruszenia danych osobowych, które może wywrzeć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną (ust. 4). Ponadto na potrzeby ujednolicenia informacji przekazywanych Generalnemu Inspektorowi Ochrony Danych Osobowych oraz abonentom lub użytkownikom końcowym, doprecyzowano katalog informacji, jakie powinny się znaleźć w zawiadomieniach kierowanych do tych podmiotów.

Wprowadzenie art. 174b ustawy Prawo telekomunikacyjne jednoznacznie przesądziło, że do sprawowanej przez GIODO kontroli wykonywania przez dostawcę publicznie dostępnych usług telekomunikacyjnych obowiązków określonych w art. 174 a i 174d, stosuje się odpowiednio przepisy ustawy o ochronie danych osobowych.

Art. 174c ustawy Prawo telekomunikacyjne stanowi implementację art. 4 ust. 4 oraz art. 4 ust. 1a akapit 2 zmienionej dyrektywy o prywatności. Na podstawie art. 174c Generalny Inspektor Ochrony Danych Osobowych może występować, zgodnie z art. 19a ust. 1 ustawy o ochronie danych osobowych, do dostawców publicznie dostępnych usług

telekomunikacyjnych, wskazując okoliczności, formę i sposób, w jaki uczestnicy rynku telekomunikacyjnego powinni uzyskać określone informacje o naruszeniu. Jednocześnie wprowadzono możliwość publikowania przez GIODO powyższych wystąpień na swojej stronie podmiotowej BIP, o ile nie będą one zawierać informacji stanowiących tajemnicę przedsiębiorstwa.

Natomiast przepis art. 174d stanowi implementację art. 4 ust. 4 akapit 2 dyrektywy o prywatności. Nakłada on na dostawcę publicznie dostępnych usług telekomunikacyjnych obowiązek prowadzenia rejestru naruszeń danych osobowych oraz określa katalog informacji, które taki rejestr powinien zawierać. Przewiduje również możliwość powierzenia przez dostawcę, w drodze umowy, prowadzenia rejestru innemu przedsiębiorcy.

2. Reforma ochrony danych osobowych w Unii Europejskiej

Doświadczenia wynikające ze stosowania przepisów o ochronie danych osobowych w Unii Europejskiej, w obliczu nowych wyzwań wynikających z technicznych uwarunkowań przetwarzania danych w Internecie oraz pojawienia się nowych kategorii danych, takich jak dane geolokalizacyjne, profile użytkowników Internetu jako konsumentów czy adresy IP, nie tylko podważyły w praktyce dotychczasowe znaczenie podstawowych pojęć w dziedzinie ochrony danych osobowych, ale stały się również przyczynkiem do rewizji obowiązujących uregulowań pod kątem gwarancji ochrony prywatności i danych osobowych.

W analizowanym 2013 roku Generalny Inspektor Ochrony Danych Osobowych kontynuował prace związane z reformą unijnych przepisów o ochronie danych osobowych, zapoczątkowane z chwilą ogłoszenia w dniu 4 listopada 2010 r. przez Komisję Europejską komunikatu do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów po nazwą „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”[3]. Celem przedmiotowej propozycji był przegląd obecnych ram prawnych oraz wypracowanie kompleksowych i spójnych rozwiązań gwarantujących pełne poszanowanie podstawowego prawa osób fizycznych do ochrony dotyczących ich danych osobowych w UE oraz poza jej granicami. Działanie to było odpowiedzią na wyzwania związane z rozwojem nowoczesnych technologii informatycznych

[3] Wniosek Komisji Europejskiej COM (2010) 609 wersja ostateczna.

i procesami globalizacji. W dniu 25 stycznia 2012 r. Komisja Europejska przedstawiła w Brukseli projekt kompleksowej reformy unijnych przepisów o ochronie danych, w celu wzmocnienia ochrony autonomii informacyjnej jednostki w Internecie oraz tworzenia warunków dla rozwoju gospodarki cyfrowej w Europie. W oparciu o ten pakiet Rada UE i Parlament Europejski rozpoczęły realizację odpowiednich procedur w ramach procesu legislacyjnego.

Planowane działania przewidują zastąpienie dyrektywy 95/46/WE **rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych (tzw. ogólne rozporządzenie o ochronie danych)**[4], które 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 przepływu danych. Projektowane zmiany przewidują również uchwalenie **dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania przestępstw i ścigania ich sprawców lub wykonywania sankcji karnych i swobodnego przepływu tych danych**[5]**.**

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. Prace nad projektem ogólnego rozporządzenia o ochronie danych, w ramach Rady UE, toczą się na forum Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (JHA), zaś na poziomie roboczym – w ramach Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (DAPIX) i grupy Przyjaciół Prezydencji ds. Ochrony Danych Osobowych. Generalny Inspektor Ochrony Danych Osobowych aktywnie uczestniczy w posiedzeniach wspomnianych grup roboczych Rady UE.

Reforma unijnych przepisów dotyczących ochrony danych osobowych była głównym tematem wywiadów udzielonych przez GIODO korespondentom polskich mediów w Brukseli podczas obchodów VII Dnia Ochrony Danych Osobowych. W dniu 28 stycznia 2013 r. mijał bowiem rok od uroczystej prezentacji założeń reformy unijnych przepisów dotyczących

[4] Wniosek Komisji Europejskiej COM (2012) 11 wersja ostateczna.
[5] Wniosek Komisji Europejskiej COM (2012) 10 wersja ostateczna.

ochrony danych osobowych. Intensywne prace, jakie trwają nad nią w Parlamencie Europejskim, wchodzą teraz w kolejną fazę. Po serii spotkań uzgodnieniowych poseł sprawozdawca unijnego rozporządzenia o ochronie danych osobowych przedstawił propozycje poprawek, jakie powinny być uwzględnione w tym dokumencie.

Projekt ogólnego rozporządzenia podlega ciągłym modyfikacjom w oparciu o zgłaszane przez państwa członkowskie uwagi. W 2013 r. prace nad tym dokumentem toczyły się bardzo intensywnie i obecny kształt projektu rozporządzenia w wersji wypracowanej przez Radę znacząco odbiega od projektu przedstawionego przez Komisję Europejską w styczniu 2012 r. Europejscy Rzecznicy Ochrony Danych pozytywnie ocenili zaproponowane w nowych przepisach kierunki zmian, np. w 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, umożliwiającym prawidłowe wykonywanie powierzonych im zadań zarówno na szczeblu krajowym, jak i w toku wzajemnej współpracy[6]. Niemniej jednak jeszcze wiele innych kwestii wymagało doprecyzowania, aby możliwe było zachowanie równowagi pomiędzy niekwestionowanymi prawami jednostki a warunkami wzrostu gospodarczego.

Prace prowadzone w 2013 r. nad projektem ogólnego rozporządzenia zmierzały do wyeliminowania nieostrych pojęć oraz wątpliwości interpretacyjnych, dotyczących w szczególności technicznej wykonalności prawa do bycia zapomnianym, zwiększenia wymogów względem administratorów danych, stosowania i egzekwowania zasad dotyczących profilowania, możliwości egzekwowania zasad dotyczących przetwarzania danych osobowych dzieci, sytuacji poważnej nierówności między podmiotem danych a administratorem, rozszerzenia definicji danych osobowych (uznanie za dane osobowe wszelkich informacji dotyczących podmiotu danych, a zatem również identyfikatory sieciowe), wyjaśnienia terminów o wysokim stopniu ogólności, jak np. „funkcje sądowe" czy „rzeczywiste działania sądowe", zasad prowadzenia działalności związanej ze stosowaniem marketingu bezpośredniego i samym charakterem takiego marketingu, zasad transferu danych osobowych do krajów trzecich, w szczególności w celach związanych z bezpieczeństwem publicznym i egzekwowaniem prawa, możliwości określenia za pomocą aktów delegowanych

[6] W tym kontekście wskazuje się, że istotną rolę odegrać może Grupa Robocza Art. 29, która ma zostać przekształcona w Europejską Radę Ochrony Danych Osobowych.

środków technicznych i organizacyjnych bezpiecznego przetwarzania danych dla konkretnych sektorów i okoliczności przetwarzania danych, czy możliwości stosowania przez państwa członkowskie licznych odstępstw od ogólnych zasad określonych w tym projekcie. Dyskutowana też była istotna z punktu widzenia ochrony autonomii informacyjnej jednostki, kwestia warunków udzielenia zgody podmiotu danych na przetwarzanie dotyczących go danych osobowych. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych konieczne jest utrzymanie wymogu udzielenia zgody w sposób „wyraźny". Oznacza to, że zgoda nie powinna być wywodzona pośrednio z zachowania danej osoby (jako tzw. zgoda kontekstowa).

Prace Rady UE koncentrowały się także wokół zagadnienia sankcji administracyjnych. Projekt rozporządzenia zobowiązuje każdy organ nadzorczy do nakładania sankcji administracyjnych, wymienionych w katalogu zawartym w przepisie art. 79, w postaci grzywien, z należytym uwzględnieniem każdego indywidualnego przypadku. Organ ds. ochrony danych osobowych zwracał uwagę na nadmierną restrykcyjność, wysokość sankcji oraz nieadekwatność do zakresu naruszeń, podkreślając potrzebę zapewnienia ich proporcjonalności. Postulował nadanie krajowym organom nadzorczym większej elastyczności w zakresie wysokości kar oraz możliwości stosowania alternatywnych środków.

Wiele szczegółowych propozycji analizowanego rozporządzenia było i wciąż jest przedmiotem dyskusji i podlega zmianom w kolejnych wersjach projektu. Analizie przebiegu prac nad reformą unijnych przepisów poświęcone było spotkanie GIODO z Françoise Le Bail, Dyrektor Generalną ds. Sprawiedliwości Komisji Europejskiej, które odbyło się w dniu 1 marca 2013 r. w Warszawie. Podczas tego spotkania poruszane były kwestie, które w toczącej się debacie wywołują największe kontrowersje lub mają istotne znaczenie dla przyszłego kształtu przepisów o ochronie danych osobowych w Europie.

W poszukiwaniu najskuteczniejszych rozwiązań Generalny Inspektor Ochrony Danych Osobowych podejmował również szereg innych działań na szczeblu krajowym (konferencje, seminaria, konsultacje z organizacjami pozarządowymi i przedstawicielami biznesu), wsłuchując się w zgłaszane przez nich wątpliwości związane z kształtem konkretnych rozwiązań przewidzianych przez ten projekt oraz by przedyskutować różne propozycje.

Planom ukształtowania nowego modelu ochrony prywatności i danych osobowych w Unii Europejskiej poświęcone były spotkania i konsultacje Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami PKPP Lewiatan (15.01.2013 r.), środowiska

marketingu bezpośredniego (17.01.2013 r.), a także z prezesami sądów, dyrektorami, sędziami i pracownikami sądów oraz prokuratorami z obszaru apelacji wrocławskiej (12.02.2013 r.). Omówieniu stanu prac nad ogólnym rozporządzeniem oraz implementacji Forein Account Tax Compliance (FATCA) poświęcone było wystąpienie GIODO podczas seminarium „Kierunki zmian w europejskim prawie dotyczącym ochrony danych osobowych i ich wpływ na sektor bankowy", którego organizatorem był Związek Banków Polskich (13.02.2013 r.). Również podczas spotkania GIODO z przedstawicielami Krajowej Izby Gospodarczej oraz niektórych izb regionalnych (19.03.2013 r.) omawiane były najważniejsze założenia projektowanej reformy w kontekście działalności podmiotów gospodarczych. Ponadto w Senacie odbyło się połączone posiedzenie Komisji Praw Człowieka, Praworządności i Petycji oraz Komisji Spraw Unii Europejskiej, zorganizowane we współpracy z Generalnym Inspektorem Ochrony Danych Osobowych (16.04.2013 r.). Podczas tej senackiej debaty z udziałem reprezentantów Parlamentu, urzędów centralnych, fundacji i stowarzyszeń, omówione zostały główne kierunki zmian regulacji ochrony danych osobowych w UE, wpływ projektu ogólnego rozporządzenia na sytuację polskich przedsiębiorców i konsumentów oraz jego relacja do przepisów krajowych, w świetle wyzwań globalizacji i współczesnych modeli biznesowych.

Podkreślenia wymaga, że w Polsce w pracach nad ogólnym rozporządzeniem wiodące jest Ministerstwo Administracji i Cyfryzacji (MAiC), które współpracuje z Generalnym Inspektorem Ochrony Danych Osobowych. W dniu 4 kwietnia 2013 r. w siedzibie Ministerstwa odbyła się dyskusja nt. reformy ochrony danych, z udziałem GIODO oraz przedstawicieli Komisji Europejskiej, Stałego Przedstawicielstwa RP przy UE, posłów do Parlamentu Europejskiego, przedstawicieli ministerstw i urzędów centralnych, a także reprezentantów organizacji pozarządowych, biznesu, środowiska naukowego oraz niezależnych ekspertów. Podobne spotkanie poświęcone reformie odbyło się w dniu 13 maja 2013 r. w ramach debaty „Cyfrowa tożsamość. Kim jesteśmy w Internecie i jak dzielimy się wiedzą o sobie?" Gościem specjalnym tego spotkania była Komisarz Viviane Reding, wiceprzewodnicząca KE, kierująca pracami nad projektem nowego rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie ochrony danych osobowych oraz odpowiedniej dyrektywy dotyczącej przetwarzania danych przez organy ścigania i wymiaru sprawiedliwości.

Stanowisko polskiego organu ds. ochrony danych osobowych wobec proponowanych zmian w projekcie ogólnego rozporządzenia o ochronie danych osobowych, ustalenie kwestii, które wymagają dalszej pracy, jeśli chodzi o przyszłość polskiego prawa o ochronie danych osobowych, a także omówienie planowanych konferencji i innych wydarzeń związanych z tą tematyką, było również przedmiotem obrad Rady Naukowej GIODO, na spotkaniu w dniu 20 listopada 2013 r.

Zagadnienia budowy nowych ram prawnych ochrony danych osobowych oraz edukacja obywateli w zakresie proponowanych regulacji dotyczących obrotu informacją w UE, pozostawały wysoko na liście priorytetów działalności GIODO w 2013 r.

3. Biuro Generalnego Inspektora Ochrony Danych Osobowych

3.1. Struktura organizacyjna

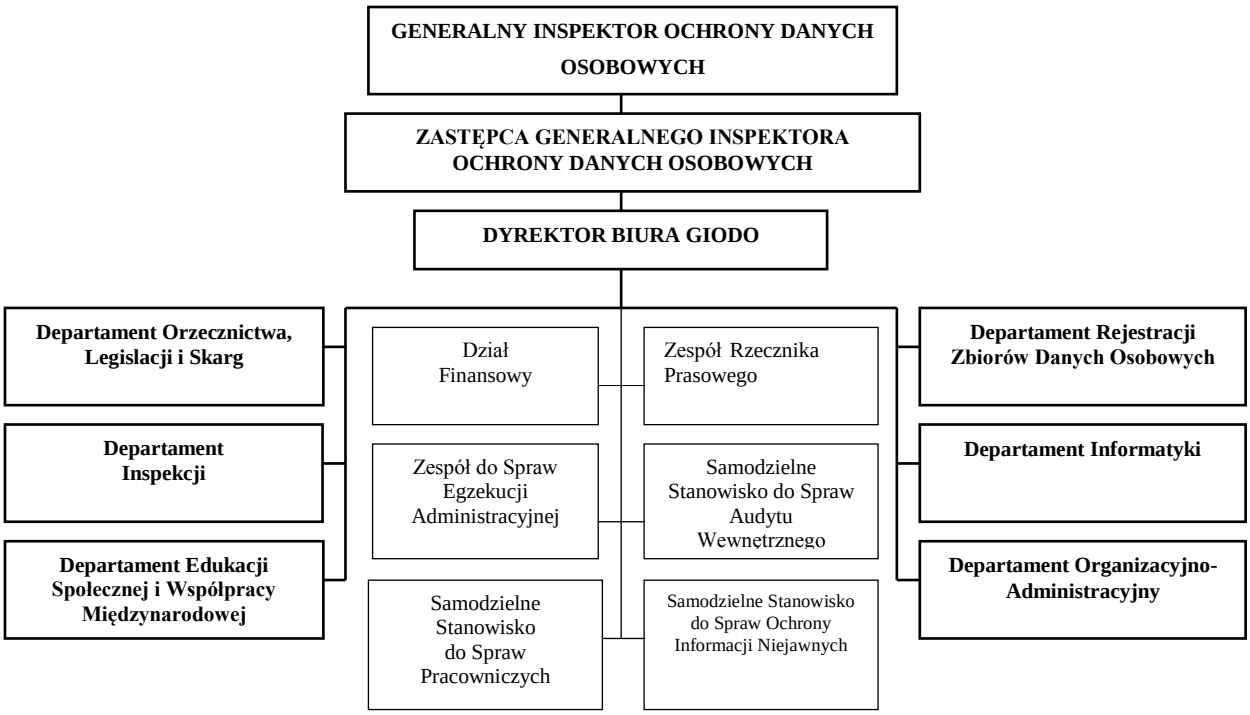
Zgodnie z art. 13 ust. 1 ustawy o ochronie danych osobowych, Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. Tryb pracy Biura, a także organizację wewnętrzną i szczegółowy zakres zadań statutowych jednostek organizacyjnych oraz jednostek zamiejscowych 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 Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. 2011, Nr 225, poz. 1350). Na mocy tego aktu powstała nowa jednostka organizacyjna Biura GIODO – Zespół do Spraw Egzekucji Administracyjnej (ZEA), a także ustalone zostały siedziby oraz właściwość miejscowa jednostek zamiejscowych, które jeszcze nie zostały powołane do życia:

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[7].

[7] 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.

3.2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO w przeliczeniu na pełne etaty wynosił na dzień 1 stycznia 2013 r. – 122,36 etatów, zaś na dzień 31 grudnia 2013 r. – 130,85 etatów. Na stanowiskach merytorycznych zatrudnionych było 119 osób, a na stanowiskach pomocniczych 16 osób. Wyższe wykształcenie posiadało 113 pracowników, w tym 75 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2013 r. przedstawia się następująco:

- GIODO - 1 osoba (1 etat)
- Zastępca GIODO – 1 osoba (1 etat)
- Dyrektor Biura – 1 osoba (1 etat)
- Zespół Rzecznika Prasowego (ZRP) – 5 osób (5 etatów)
- Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) – 10 osób (9,75 etatu),
- Departament Informatyki (DIF) – 15 osób (15 etatów),
- Departament Inspekcji (DIS) – 14 osób (14 etatów),
- Departament Organizacyjno-Administracyjny (DOA) – 19 osób (17,90 etatu),
- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 37 osób (37 etatów),
- Departament Rejestracji Zbiorów Danych Osobowych (DRZDO) – 18 osób (17,875 etatów),
- 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).

3.3. Budżet Generalnego Inspektora Ochrony Danych Osobowych za 2013 rok

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2013 r. wynosił: **15 060** tys. zł, w tym:

- wynagrodzenia 9 351 tys. zł

- pochodnie od wynagrodzeń 1 690 tys. zł
- wydatki majątkowe 473 tys. zł
- pozostałe wydatki 3 546 tys. zł

Wydatki zrealizowane przez GIODO w 2013 roku w kwocie **14 989** tys. zł obejmowały:

- wynagrodzenia 9 319 tys. zł
- pochodne od wynagrodzeń 1 688 tys. zł
- wydatki majątkowe 472 tys. zł
- pozostałe wydatki 3 510 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[8]. Z jego treści wynika, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a co za tym idzie, ma on przestrzegać wskazanych poniżej zasad:

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

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

[8] 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.

Podsumowując należy stwierdzić, że 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 osobowych 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 w oparciu o art. 12 pkt 1 i art. 14 ustawy o ochronie danych osobowych. W art. 14 tej 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 przywołanym art. 12 pkt 1.

Uprawnienia te obejmują w szczególności prawo wstępu do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą, żądania złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania osób w zakresie niezbędnym do ustalenia stanu faktycznego, wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii, przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych, a także zlecania 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 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 2013 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **173 kontrole** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych.

2.2.1. Administracja publiczna

W 2013 r. w podmiotach wykonujących zadania publiczne przeprowadzono **30 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W ramach tej kategorii podmiotów kontrole przeprowadzono m.in. w 15 jednostkach samorządu terytorialnego w związku z realizacją obowiązków wynikających z ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. z 2012 r. poz. 391 z późn. zm.).

Wypełniając obowiązek wynikający z art. 6m ust. 1^9 i art. 6n ust. 1 pkt 1^{10} ustawy o utrzymaniu czystości i porządku w gminach, rady gminy określiły wzory deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, w których osoba składająca deklarację obowiązana jest podać m.in. swoje dane osobowe. W niektórych przypadkach rady miejskie określając wzór ww. deklaracji, zobligowały osoby wypełniające deklarację do podawania zbyt szerokiego zakresu danych osobowych, nieadekwatnego do celu ich przetwarzania. W toku przeprowadzonych kontroli stwierdzono, iż oprócz imienia i nazwiska, numeru PESEL, adresu zamieszkania i adresu nieruchomości, której dotyczy deklaracja, pozyskiwano dane osobowe właścicieli nieruchomości w następującym zakresie: nazwisko rodowe, data urodzenia, imię ojca, imię matki, numer księgi wieczystej nieruchomości, numer geodezyjny działki oraz numer PESEL przedsiębiorcy będącego osobą fizyczną.

Gminy wskazywały, że pozyskują dane osobowe obejmujące nazwisko rodowe, datę urodzenia, imię ojca, imię matki oraz numer księgi wieczystej nieruchomości na wypadek konieczności wystawienia wobec zobowiązanego tytułu wykonawczego, w przypadku zalegania przez niego z zapłatą zobowiązania z tytułu opłaty za gospodarowanie odpadami komunalnymi, o którym mowa w rozporządzeniu Ministra Finansów z dnia 22 listopada 2001 r. w sprawie wykonania niektórych przepisów ustawy o postępowaniu egzekucyjnym w administracji (Dz. U. Nr 137, poz. 1541 z późn. zm.). Generalny Inspektor uznał, że pozyskiwanie powyższych danych osobowych oznacza gromadzenie tych danych „na zapas", w celu ich ewentualnego wykorzystania w postępowaniu egzekucyjnym, tj. wystawienia tytułu wykonawczego. Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w uzasadnieniu wyroku z dnia 1 grudnia 2005 r. (sygn. II SA/Wa 917/2005), gromadzenie danych osobowych na wypadek, gdyby w przyszłości zaszła potrzeba ich wykorzystania nie może być uznane za zgodne z przepisami o ochronie danych osobowych. Wobec powyższego uznano, iż gromadzenie danych osobowych osób składających deklarację w zakresie nazwiska rodowego, daty urodzenia, imienia ojca, imienia matki, numeru księgi wieczystej

[9] Art. 6m.1. Właściciel nieruchomości jest obowiązany złożyć do wójta, burmistrza lub prezydenta miasta deklarację o wysokości opłaty za gospodarowanie odpadami komunalnymi w terminie 14 dni od dnia zamieszkania na danej nieruchomości pierwszego mieszkańca lub powstania na danej nieruchomości odpadów komunalnych.

[10] Art. 6n.1.1. Rada gminy, uwzględniając konieczność zapewnienia prawidłowego obliczenia wysokości opłaty za gospodarowanie odpadami komunalnymi oraz ułatwienia składania deklaracji, określi w drodze uchwały stanowiącej akt prawa miejscowego wzór deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanej przez właścicieli nieruchomości, obejmujący objaśnienia dotyczące sposobu jej wypełnienia oraz pouczenie, że deklaracja stanowi podstawę do wystawienia tytułu wykonawczego.

nieruchomości jest nieadekwatne do celu przetwarzania tych danych, którym jest identyfikacja osoby składającej deklarację, co stanowi naruszenie art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych[11].

Jedna z gmin pozyskiwała za pośrednictwem deklaracji numer geodezyjny działki w celu, jak wskazywała, jednoznacznej identyfikacji nieruchomości, której dotyczyła deklaracja. Jak jednak ustalono, informacje dotyczące adresu nieruchomości pozyskiwane za pośrednictwem deklaracji w zakresie: miejscowość, ulica, numer budynku i numer lokalu są niewątpliwie wystarczające dla stwierdzenia, której nieruchomości dotyczy deklaracja i pozyskiwanie w tym celu informacji w zakresie numeru geodezyjnego działki Generalny Inspektor uznał za zbędne i wykraczające poza cel przetwarzania danych osobowych zawartych w deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, a tym samym naruszające art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Natomiast inna gmina pozyskiwała za pomocą wspomnianej deklaracji dane w zakresie imienia, nazwiska i nr PESEL w celu identyfikacji osób zamieszkujących nieruchomość, za które właściciel tej nieruchomości był zobowiązany uiszczać opłatę za gospodarowanie odpadami komunalnymi. Również w tym przypadku Generalny Inspektor uznał, że dla osiągnięcia celu, jakim jest prawidłowe naliczenie opłaty za gospodarowanie odpadami komunalnymi, wystarczające jest pozyskanie wyłącznie informacji o liczbie osób zamieszkujących tę nieruchomość, bez zbierania szczegółowych danych dotyczących poszczególnych osób. Przetwarzanie wskazanych danych było zatem nieadekwatne do celu ich przetwarzania i naruszało art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Zgodnie z przepisami ustawy o utrzymaniu czystości i porządku w gminach, spółdzielnia mieszkaniowa jest zobligowana do złożenia deklaracji o wysokości opłat za gospodarowanie odpadami komunalnymi. Poprawne złożenie deklaracji wymagało ustalenia rzeczywistej liczby mieszkańców zarządzanych lokali, bądź będących w zasobie spółdzielni (rozumianej przez przepisy ww. ustawy jako właściciela nieruchomości). W spółdzielni opracowano wzór oświadczenia, w którym właściciel lokalu (osoba uprawniona) był zobowiązany podać imiona, nazwiska, nr PESEL osób zamieszkujących w lokalu.

[11] Art. 26 ust. 1 pkt 3 administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

Jak ustalono, powyższe dane spółdzielnia zbierała w celu zapewnienia możliwości dochodzenia roszczeń z tytułu opłat za odbiór odpadów komunalnych także od osób zamieszkujących w lokalu. Jest to związane z faktem, iż spółdzielnia ponosi odpowiedzialność za uiszczenie opłaty za gospodarowanie odpadami komunalnymi w należnej wysokości, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. z 2012 r. poz. 749 z późn. zm.), zaś zgodnie z art. 4 ust. 6 ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2003 r. Nr 119, poz. 1116 z późn. zm.), za opłaty, o których mowa w ust. 1-2 i 4, odpowiadają solidarnie z członkami spółdzielni, właścicielami lokali niebędącymi członkami spółdzielni lub osobami niebędącymi członkami spółdzielni, którym przysługują spółdzielcze własnościowe prawa do lokali, osoby pełnoletnie stale z nimi zamieszkujące w lokalu, z wyjątkiem pełnoletnich zstępnych pozostających na ich utrzymaniu, a także osoby faktycznie korzystające z lokalu. Przy czym opłaty, o których mowa w tym przepisie, to przede wszystkim koszty związane z eksploatacją i utrzymaniem nieruchomości w częściach przypadających na poszczególne lokale, eksploatacją i utrzymaniem nieruchomości stanowiących mienie spółdzielni. Ponadto spółdzielnia wskazała, że numer PESEL, zgodnie z aktualizacją przepisów Kodeksu postępowania cywilnego, jest informacją niezbędną do wszczęcia postępowania nakazowego w e-sądzie[12]. Biorąc pod uwagę powyższe uznano, że dane osobowe pozyskiwane w związku z odbieraniem przez spółdzielnię wskazanego oświadczenia, nie były adekwatne w stosunku do celu ich pozyskiwania, którym było złożenie deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi. Informacje te gromadzone były „na zapas", w celu ich ewentualnego wykorzystania w postępowaniach windykacyjnych i egzekucyjnych. Dlatego też przetwarzanie danych osobowych w zakresie imienia, nazwiska, nr PESEL osób zamieszkujących w lokalu, jako nieadekwatnych w stosunku do celu w jakim są przetwarzane, narusza art. 26 ust. 1 pkt 3 ustawy.

W analizowanym roku sprawozdawczym przeprowadzono również kontrolę w dwóch spółkach, które wygrały przetarg na odbiór odpadów komunalnych w jednej z gmin i podpisały z tą gminą stosowne umowy.

[12] Na podstawie ustawy z dnia 10 maja 2013 r. o zmianie ustawy – Kodeks postępowania cywilnego (Dz. U. z 2013 r. poz. 654), zmianie uległ m.in. art. 505^{32} § 2 Kodeksu postępowania cywilnego, w zakresie obowiązku podania numeru PESEL pozwanego w pozwie składanym w elektronicznym postępowaniu upominawczym. Przedmiotowa zmiana weszła w życie 7 lipca 2013 r.

W związku z wykonywaniem ww. umów, spółki przetwarzały następujące informacje: dane dotyczące adresu nieruchomości, z której odbierane były odpady komunalne (liczba mieszkańców, adres: kod pocztowy, miejscowość, numer domu, numer mieszkania) oraz informacje dotyczące odbioru odpadów komunalnych (m.in. rodzaj i ilość pojemników, częstotliwość odbiorów odpadów). Powyższe informacje uznano za dane osobowe w myśl art. 6 ustawy, a w konsekwencji umowy te zakwalifikowano jako umowy, którymi gmina powierzyła, zgodnie z art. 31 ust. 1 ustawy o ochronie danych osobowych, przetwarzanie ww. danych osobowych.

Spółki te wdrożyły i wykorzystywały system elektronicznego ewidencjonowania i potwierdzania odbioru poprzez przypisanie unikalnych numerów identyfikacyjnych do danego punktu wywozowego (nieruchomość). Oznaczyły też pojemniki przeznaczone na odpady komunalne z wykorzystaniem elektronicznych identyfikatorów posiadających zakodowane informacje dotyczące unikalnego numeru identyfikacyjnego pojemnika (chip z zakodowanymi informacjami służącymi do identyfikacji pojemników na odpady komunalne na danej nieruchomości). Właścicielom nieruchomości zabudowanych budynkami mieszkalnymi jednorodzinnymi dostarczane były przez spółki wydrukowane etykiety adresowe zawierających kody kreskowe, które naklejone na worki do gromadzenia odpadów służyły identyfikacji odbioru odpadów, ich ilości oraz rodzaju. Na etykiecie adresowej naklejanej na worek znajdowały się następujące informacje: dane spółki (nazwa, siedziba, numer telefonu), rodzaj frakcji (zielona, sucha) oraz kod kreskowy z numerem.

W toku kontroli[13] przeprowadzonej w jednym z urzędów miast ustalono, że prezydent miasta nie zgłaszał do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osób fizycznych i osób fizycznych prowadzących działalność gospodarczą przetwarzanych w związku ze składaniem deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi kierując się tym, że zbiór taki został zgłoszony do rejestracji przez jednostkę organizacyjną gminy miejskiej, działającą w formie jednostki budżetowej. W celu sprawniejszej realizacji spoczywających na gminie nowych obowiązków wynikających z ustawy o utrzymaniu czystości i porządku w gminach[14], przeniesiono kompetencje funkcjonującego w urzędzie miasta wydziału do ww. jednostki organizacyjnej gminy, gdzie

[13] Sygn. kontroli: DIS-K-421/121/13
[14] ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. z 2012 r. Nr 391 z późn. zm.).

utworzono komórkę zajmującą się kwestią gospodarki odpadami. Prezydent miasta wykorzystał tym samym upoważnienie rady miasta określone w treści statutu ww. jednostki organizacyjnej gminy, do zlecenia tej jednostce zadań z zakresu administracji publicznej (w tym przypadku wykonywanie obowiązków wynikających z ustawy o utrzymaniu czystości i porządku w gminach). Upoważnienie to znajduje oparcie w art. 39 ust. 4 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r. poz. 594 z późn. zm.), zgodnie z którym rada gminy może upoważnić również organ wykonawczy jednostki pomocniczej oraz jednostek i podmiotów, o których mowa w art. 9 ust. 1 ww. ustawy (a więc również ww. jednostkę organizacyjną gminy), do załatwiania indywidualnych spraw z zakresu administracji publicznej. W związku z tym, że w toku kontroli ustalono, że rada miasta powierzyła wykonanie uchwał przyjętych w związku z realizacją zadań własnych miasta wynikających z ustawy o utrzymaniu czystości i porządku w gminach prezydentowi miasta, o czym stanowi ich treść, w opisanym stanie faktycznym i prawnym podjęto decyzję o poinformowaniu prezydenta miasta, że administratorem danych osobowych mieszkańców miasta przetwarzanych w związku z realizacją przedmiotowej ustawy jest prezydent miasta i z tego powodu obowiązek zgłoszenia do rejestracji Generalnemu Inspektorowi zbioru danych osób fizycznych i osób fizycznych prowadzących działalność gospodarczą przetwarzanych w związku ze składaniem deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi ciąży bezpośrednio na tymże organie gminy, a nie na ww. jednostce organizacyjnej gminy.

Na podstawie dokonanych ustaleń należy stwierdzić, że większość z kontrolowanych gmin wprowadziła deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi, które nakładały na składających deklaracje obowiązek podawania także tych danych osobowych, których przetwarzanie było nieadekwatne do celu ich przetwarzania.

Natomiast pozostałe stwierdzone w toku kontroli uchybienia dotyczyły głównie nieprawidłowości w systemach informatycznych i polegały na naruszeniu następujących obowiązków wynikających z przepisów o ochronie danych osobowych, tj. m.in.: braku odpowiedniego zabezpieczenia wypełnionych deklaracji (art. 36 ust. 1 ustawy), braku wymaganych elementów w polityce bezpieczeństwa (art. 36 ust. 2 ustawy w związku z § 4 pkt 1, pkt 2, pkt 3 rozporządzenia), braku zapewnienia dla każdej osoby, której dane osobowe były przetwarzane w systemie informatycznym, sporządzenia i wydrukowania raportu

zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1 (art. 38 ustawy w związku z § 7 ust. 3 rozporządzenia).

W przypadkach stwierdzenia, iż za pomocą deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi pozyskiwane były dane osobowe, które to działanie zostało uznane za nieadekwatne do celu ich przetwarzania, na podstawie art. 19a ust. 1 ustawy[15] GIODO zwracał się do rad gmin z prośbą o podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, w zakresie zapewnienia zgodności wzoru deklaracji z przepisami o ochronie danych osobowych.

W podmiotach, w których stwierdzono uchybienia dające podstawę do zastosowania środków, o których mowa w art. 18 ust. 1 ustawy[16], wobec administratorów danych wszczęte zostały postępowania administracyjne oraz wydane zostaną decyzje nakazujące usunięcie uchybień lub decyzje umarzające postępowanie, jeżeli uchybienia zostaną usunięte w toku prowadzonych postępowań.

Kontrole w związku z realizacją obowiązków wynikających z ustawy o utrzymaniu czystości i porządku w gminach nie były jednak jedynymi, które zostały przeprowadzone w okresie sprawozdawczym w podmiotach wykonujących zadania publiczne. Na uwagę zasługuje kontrola jednego z urzędów miasta[17]. W jej toku ustalono, że w procesie przetwarzania danych osobowych prezydent tego miasta naruszył przepisy o ochronie danych osobowych poprzez udostępnianie zarządowi dróg miejskich w tym mieście (dalej: „ZDM"), w związku z prowadzonymi przez ten podmiot postępowaniami windykacyjnymi, danych osobowych w szerszym zakresie niż wynikało to z wniosku ZDM o udostępnienie tych danych. Jak ustalono, ZDM wystąpił do urzędu miasta z wnioskiem o udostępnienie danych osób zobowiązanych do wniesienia opłaty dodatkowej za nieuiszczenie opłaty za parkowanie

[15] Art. 19a. 1. W celu realizacji zadań, o których mowa w art. 12 pkt 6, Generalny Inspektor 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.

[16] 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, zabezpieczenie danych lub przekazanie ich innym podmiotom, usunięcie danych osobowych.

[17] Kontrola DIS-K-421/98/13

w tzw. „strefie płatnego parkowania niestrzeżonego”[18]. Wniosek dotyczył danych ww. osób w zakresie: imię, nazwisko, PESEL, adres zameldowania na pobyt stały i czasowy. W odpowiedzi na ww. wniosek wybranym pracownikom ZDM umożliwiono dostęp do systemu informatycznego, w którym prezydent miasta przetwarza dane osobowe gromadzone na podstawie art. 44a ust. 1 pkt 1 oraz art. 44e 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.)[19]. Pracownicy ZDM za pośrednictwem ww. systemu informatycznego mieli dostęp do informacji o osobach zobowiązanych do wniesienia opłaty dodatkowej za nieuiszczenie opłaty za parkowanie w „strefie płatnego parkowania niestrzeżonego” między innymi takich jak: imię, nazwisko, nazwisko rodowe, PESEL, obywatelstwo, imiona i nazwiska rodowe ojca i matki, adres, data i miejsce urodzenia, informacje o stanie cywilnym i informacje o współmałżonku (np. imię, nazwisko, PESEL). Ich zakres był zatem szerszy niż wynikało to z wniosku ZDM. Jednocześnie dane te wykraczały poza zakres danych identyfikacyjnych zobowiązanego wskazanych we wzorze tytułu wykonawczego, który został wprowadzony rozporządzeniem Ministra Finansów z dnia 22 listopada 2001 r. w sprawie wykonania niektórych przepisów ustawy o postępowaniu egzekucyjnym w administracji (Dz. U. z 2001 r. Nr 137, poz. 1541)[20]. Generalny Inspektor uznał zatem, iż udostępnianie ZDM danych osobowych identyfikujących zobowiązanego w zakresie szerszym niż wynika to z wzoru tytułu wykonawczego było nieadekwatne w stosunku do celu, w jakim były one przetwarzane. Tym samym doszło tu do naruszenia przez prezydenta miasta art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych[21].

[18] Opłata dodatkowa za parkowanie w „strefie płatnego parkowania niestrzeżonego” bez wniesienia należnej opłaty nakładana jest na podstawie art. 13f ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2007 r., Nr 19, poz. 115).

[19] Na podstawie przepisów ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (t.j. Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.) prowadzony jest m.in. zbiór meldunkowy, o którym mowa w art. 44a ust. 1 pkt 1 ww. ustawy oraz ewidencja wydanych i unieważnionych dowodów osobistych, o której mowa w art. 44e ust. 1. ww. ustawy.

[20] Art. 40d ust. 2 ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2007 r. Nr 19, poz. 115) opłaty dodatkowe ściągane są w trybie określonym w przepisach ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji. Zatem zakres danych osobowych udostępnianych ZDM w związku z prowadzonymi przez ww. podmiot postępowaniami windykacyjnymi powinien być zgodny z zakresem danych osobowych wskazanym we wzorze tytułu wykonawczego określonym w rozporządzeniu Ministra Finansów z dnia 22 listopada 2001 r. w sprawie wykonania niektórych przepisów ustawy o postępowaniu egzekucyjnym w administracji (Dz. U. z 2001 r. Nr 137, poz. 1541).

[21] Art. 26 ust. 1 pkt 3. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

2.2.2. Bezpieczeństwo publiczne

W 2013 r. Generalny Inspektor przeprowadził **14 kontroli** dotyczących 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 Komendzie Głównej Policji, u Szefa Służby Cywilnej, Generalnego Inspektora Kontroli Skarbowej, w Urzędzie do Spraw Cudzoziemców, w jednostce Straży Granicznej, urzędzie kontroli skarbowej, urzędzie skarbowym, jednostkach Służby Celnej (4 kontrole) oraz w konsulatach przy ambasadach Rzeczypospolitej Polskiej (3 kontrole)[22].** 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.

Do najważniejszych w tym zakresie należała kontrola przeprowadzona w Centralnym Organie Technicznym KSI (którym zgodnie z art. 2 pkt 3 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym jest Komendant Główny Policji[23]) na wniosek Komendanta Głównego Policji w związku z dokonywanymi zmianami w KSI polegającymi na uruchomieniu Systemu Informacyjnego Schengen drugiej generacji (SIS II). Wskazany wniosek został złożony w trybie art. 34 ust. 1 ww. ustawy[24]. W wyniku ustaleń kontroli przeprowadzonej w Komendzie Głównej Policji Generalny Inspektor wydał pozytywną opinię w zakresie zmian wprowadzonych w KSI

[22] Np. kontrole DIS-K-421/27/13, DIS-K-411/34/13, DIS-K-411/97/13, DIS-K-411/126/13, DIS-K-421/148/13.

[23] Art. 2 pkt 3. Ilekroć w ustawie jest mowa o centralnym organie technicznym KSI - rozumie się przez to Komendanta Głównego Policji.

[24] Art. 34. 1. W przypadku dokonywania jakichkolwiek zmian w Krajowym Systemie Informatycznym (KSI) po jego uruchomieniu centralny organ techniczny KSI jest obowiązany przed wdrożeniem tych zmian do uzyskania pisemnej opinii ministra właściwego do spraw wewnętrznych w zakresie spełniania przez Krajowy System Informatyczny (KSI) wymogów określonych w art. 4 i 9 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz w art. 4 i 9 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), oraz opinii Generalnego Inspektora Ochrony Danych Osobowych.

uznając, iż spełnione zostały wymogi określone w art. 36-39 ustawy z dnia o ochronie danych osobowych oraz w przepisach wydanych na podstawie art. 39a tej ustawy.

Pozostałe kontrole przeprowadzone w podmiotach mających dostęp do danych SIS i / lub danych VIS, w większości przypadków nie wykazały uchybień w zakresie przestrzegania przepisów ochronie danych osobowych. Jedynie w toku kontroli przeprowadzonych w konsulatach, jednostkach Służby Celnej, u Generalnego Inspektora Kontroli Skarbowej oraz Urzędzie do Spraw Cudzoziemców stwierdzono nieprawidłowości w zakresie prowadzonej dokumentacji przetwarzania danych osobowych. Polegały one m.in. na nieuwzględnieniu systemu WWW VIS w wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, niezawarciu informacji opisujących zastosowane środki techniczne i organizacyjne zapewniające poufność przetwarzanych danych VIS oraz zastosowane środki techniczne i organizacyjne mające na celu ochronę przed nieuprawnionym dostępem do obszarów i pomieszczeń, w których przetwarzane będą dane VIS, a także na braku opisu przepływu danych osobowych pomiędzy poszczególnymi systemami informatycznymi. Ponadto w konsulatach nie zostały opracowane pisemne procedury kontrolne wskazujące działania podejmowane w celu zapewnienia zgodności wykorzystywania danych SIS z obowiązującymi przepisami, zaś u Generalnego Inspektora Kontroli Skarbowej nie został wyznaczony administrator bezpieczeństwa informacji.

W podmiotach, w których stwierdzono uchybienia dające podstawę do zastosowania środków, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych[25], wobec administratorów danych wszczęte zostały postępowania administracyjne i wydano decyzje nakazujące usunięcie uchybień lub decyzje umarzające postępowanie, jeżeli uchybienia zostaną usunięte w toku prowadzonych postępowań. Ponadto w związku z kontrolami przeprowadzonymi w konsulatach zaistniała konieczność przeprowadzenia czynności kontrolnych w Ministerstwie Spraw Zagranicznych.

Oprócz kontroli związanych z przetwarzaniem danych osobowych w Krajowym Systemie Informatycznym (KSI) Generalny Inspektor w 2013 r. przeprowadził także kontrole

[25] 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.

w strażach gminnych. W jednej z nich[26] stwierdzono, że sprawcy wykroczeń mieli możliwość sprawdzenia za pomocą systemu informatycznego (elektronicznej platformy), na jakim etapie znajduje się sprawa dotycząca popełnionego przez nich wykroczenia prowadzona przez straż gminną. Ustalenia wykazały, iż system ten stworzony został w celu usprawnienia obsługi interesantów (sprawców wykroczeń). Komendant kontrolowanej straży gminnej zawarł z twórcą ww. systemu informatycznego, jako osobą fizyczną (będącą jednocześnie komendantem innej straży gminnej), umowę o udostępnienie straży gminnej elektronicznej platformy. Zgodnie z powołaną umową elektroniczna platforma dostępna była na serwerze zewnętrznym twórcy systemu, a podstawowa funkcjonalność tej platformy polegała na wyświetlaniu jej użytkownikowi (sprawcy wykroczenia) komunikatów o stanie sprawy, tj. numer sprawy, numer rejestracyjny pojazdu, status wykroczenia (przyznanie się do wykroczenia, wskazanie innego użytkownika lub zgoda na mandat bez wskazania sprawcy), status sprawy (mandat, przekazanie sprawy do sądu lub wystawienie tytułu wykonawczego), przekroczona prędkość. Umowa ta stanowiła umowę powierzenia przetwarzania danych, o której mowa w art. 31 ustawy o ochronie danych osobowych[27]. W toku kontroli prowadzonej przez inspektorów Biura Generalnego Inspektora Ochrony Danych Osobowych, komendant kontrolowanej straży gminnej rozwiązał ww. umowę w związku z tym, że zarówno on jak i jego pracownicy nie posiadali konta do elektronicznej platformy, a zatem możliwości sprawowania kontroli nad prawidłowością jej działania, zaś napływające wcześniej do straży gminnej sygnały od jej użytkowników (sprawców wykroczeń) dawały podstawę do uznania, iż system ten nie jest na bieżąco uaktualniany. Także wydatkowane środki finansowe na utrzymanie niesprawnie działającej platformy elektronicznej były podstawą do rozwiązania ww. umowy. Komendant straży gminnej zobowiązał twórcę systemu do usunięcia na trwałe wszystkich danych z elektronicznej platformy. W związku z tym, iż do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła od twórcy systemu informacja o tym, iż wszystkie dane sprawców wykroczeń kontrolowanej straży gminnej zostały usunięte z elektronicznej platformy, nie zostały w tym zakresie podjęte dalsze czynności w sprawie.

[26] Kontrola DIS-K-421/119/13
[27] Art. 31 ust. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

W okresie sprawozdawczym przeprowadzono również 8 kontroli w jednostkach Policji (w Komendzie Głównej Policji oraz w siedmiu terenowych jednostkach organizacyjnych Policji szczebla wojewódzkiego i powiatowego) w celu sprawdzenia, czy w testowanym przez Policję systemie informatycznym o nazwie „e-Posterunek", który miał stanowić narzędzie służące do prowadzenia w wersji elektronicznej postępowań przygotowawczych przez Policję, przetwarzane są dane fikcyjne, czy też rzeczywiste dane osób fizycznych. Z ustaleń kontroli wynika, że terenowe jednostki organizacyjne Policji otrzymały polecenie Zastępcy Komendanta Głównego Policji zawarte w piśmie z dnia 8 czerwca 2010 r. dotyczące uruchomiania systemu „e-Posterunek", w sytuacji niedopełnienia przez Komendanta Głównego Policji, jako administratora danych[28], obowiązku zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną mających na celu zabezpieczenie danych, wynikającego z art. 36 ust. 1 ustawy o ochronie danych osobowych, w szczególności w zakresie prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną mających na celu zabezpieczenie danych przetwarzanych przy użyciu systemu informatycznego o nazwie „e-Posterunek". Uchybienia w tym zakresie dotyczyły niewdrożenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, niezapewnienia przez wskazaną aplikację odnotowania daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu dla każdej osoby, której dane przetwarzane są w systemie, a także nienadania upoważnień do przetwarzania danych osobowych dla funkcjonariuszy, którzy mieli użytkować aplikację „e-Posterunek" i w związku z tym nieprowadzenia w zakresie

[28] § 3 ust. 2 rozporządzenia Ministra Spraw Wewnętrznych z dnia 31 grudnia 2012 r. w sprawie przetwarzania informacji przez Policję (Dz. U. z 2013 r., poz. 8). Komendant Główny Policji jest również administratorem danych w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych w odniesieniu do danych osobowych dotyczących osób, o których mowa w § 1 pkt 1, przetwarzanych przez Policję w zbiorach danych.

systemu „e-Posterunek” ewidencji osób upoważnionych do przetwarzania danych osobowych. Ponadto ustalono, że na kilku stanowiskach komputerowych, na których był zainstalowany system informatyczny o nazwie „e-Posterunek”, bazy programów antywirusowych były nieaktualne.

Jednocześnie na podstawie materiału dowodowego zebranego w toku przeprowadzonych czynności kontrolnych należy stwierdzić, że jednostki Policji poddane kontroli nie naruszają obecnie przepisów o ochronie danych osobowych w zakresie objętym kontrolą, ponieważ wypełniając polecenie Komendanta Głównego Policji, zawarte w piśmie z dnia 17 grudnia 2012 r. zaprzestały przetwarzania danych osobowych przy użyciu aplikacji „e-Posterunek”. Z uwagi na to, że w żadnej ze skontrolowanych jednostek Policji nie stwierdzono naruszenia przepisów o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych nie zastosował wobec podmiotów poddanych kontroli środków, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych[29].

Mając na uwadze, że system informatyczny o nazwie „e-Posterunek” może zostać w przyszłości wprowadzony do użytkowania w praktyce policyjnej, a co za tym idzie - służyć do przetwarzania danych osobowych - do Komendanta Głównego Policji zostało skierowane pismo[30] informujące o ustaleniach dokonanych w toku przeprowadzonych kontroli oraz o konieczności zapewnienia, aby w związku z opracowywaniem narzędzi informatycznych, które mają być wykorzystywane przez Policję do przetwarzania danych osobowych, były spełniane wymogi wynikające z przepisów o ochronie danych osobowych[31].

2.2.3. Służba zdrowia

W okresie sprawozdawczym w podmiotach należących do sektora służby zdrowia zostało przeprowadzonych **6 kontroli.** Do najistotniejszych należały kontrole przeprowadzone w Narodowym Funduszu Zdrowia w związku z uruchomieniem systemów

[29] 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.
[30] Pismo z dnia 20 marca 2014 r. DIS-K-421/100/13/21569/14.
[31] W 2014 r. Komendant Główny Policji podjął decyzję o niewdrażaniu systemu „e-Posterunek”. Decyzja ta nie była jednak bezpośrednio umotywowana zagadnieniami związanymi z przetwarzaniem danych osobowych.

informatycznych o nazwach Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców - eWUŚ i Zintegrowany Informator Pacjenta - ZIP [32].

Narodowy Fundusz Zdrowia rozpoczął prace nad systemem informatycznym eWUŚ w związku z nowelizacją ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2008 r. Nr 164, poz. 1027 z późn. zm.), w wyniku której wprowadzona została możliwość przeprowadzania przez świadczeniodawców elektronicznej weryfikacji uprawnień świadczeniobiorców do uzyskania świadczenia opieki zdrowotnej[33]. Świadczeniodawca, który zamierza dokonywać weryfikacji uprawnień osób ubiegających się o świadczenie opieki zdrowotnej za pomocą systemu eWUŚ, musi spełnić warunki określone w rozporządzeniu Ministra Zdrowia z dnia 28 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej (Dz. U. poz. 1500). W oparciu o ww. system upoważnieni pracownicy świadczeniodawcy kierują zapytania do NFZ o status uprawnień pacjenta do uzyskania świadczenia opieki zdrowotnej. W odpowiedzi generowana jest informacja, że NFZ potwierdza lub nie potwierdza prawa do świadczeń. Ponadto system eWUŚ może wygenerować informację o nieprawidłowym numerze PESEL (system ten jest wyposażony w funkcjonalność pozwalającą na sprawdzenie poprawności nr PESEL). Dla użytkowników ww. systemu NFZ opracował zasady postępowania w przypadku niezgodności przetwarzanych w nim danych z danymi podanymi przez osobę ubiegającą się o świadczenie opieki zdrowotnej. Zgodnie z tymi zasadami, użytkownik zobowiązany jest w takich sytuacjach do zachowania tajemnicy i nieujawniania danych znajdujących się w systemie eWUŚ oraz do poinformowania tej osoby o zaistnieniu rozbieżności w danych.

System informatyczny o nazwie Zintegrowany Informator Pacjenta - ZIP jest ogólnopolskim serwisem udostępniającym zarejestrowanym użytkownikom historyczne dane o ich leczeniu i finansowaniu leczenia, gromadzone od 2008 r. przez Narodowy Fundusz Zdrowia. Wdrożenie systemu ZIP stanowi realizację art. 192 ust. 1 i 192a ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2008 r. Nr 164, poz. 1027 z późn. zm.)[34]. Sposób, tryb oraz termin

[32] Kontrole: DIS-K-421/47/13 i DIS-K-421/112/13.
[33] Nowelizacja ta została wprowadzona w lipcu 2012 r. z mocą obowiązującą od dnia 1 stycznia 2013 r.
[34] Art. 192. 1. Fundusz na żądanie świadczeniobiorcy informuje go o: 1) posiadanym w danym dniu prawie do świadczeń opieki zdrowotnej oraz podstawie tego prawa, a w przypadku gdy prawo do świadczeń opieki zdrowotnej wynika z objęcia ubezpieczeniem zdrowotnym, także o dacie zgłoszenia do ubezpieczenia

występowania do Narodowego Funduszu Zdrowia oraz udostępniania świadczeniodawcy przez ten podmiot, informacji o prawie do świadczeń opieki zdrowotnej, udzielonych świadczeniach oraz kwocie środków finansowych wydatkowanych na sfinansowanie tych świadczeń, został określony w rozporządzeniu Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie sposobu, trybu i terminów występowania do Narodowego Funduszu Zdrowia oraz udostępniania przez Narodowy Fundusz Zdrowia świadczeniobiorcy informacji o prawie do świadczeń opieki zdrowotnej oraz o udzielonych mu świadczeniach (Dz. U. poz. 1505). Pacjent uzyskuje dostęp do tych danych po złożeniu w NFZ stosownego wniosku i osobistym odebraniu danych dostępowych do ww. systemu, tj. loginu i hasła. Użytkownik systemu ZIP w ramach swojego konta ma dostęp do informacji o świadczeniach opieki zdrowotnej zrealizowanych na jego rzecz przez świadczeniodawców, mających podpisane umowy z NFZ i finansowanych ze środków publicznych (moduł o nazwie „Rejestr usług medycznych" obejmujący informacje o wykonanych świadczeniach medycznych, leczeniu uzdrowiskowym, zrealizowanych receptach refundowanych, zrealizowanych środkach ortopedycznych, złożonych deklaracjach w POZ oraz kolejkach oczekujących, do których pacjent został wpisany), do podstawowych informacji dotyczących prawa do ochrony zdrowia oraz prawa do świadczeń opieki zdrowotnej finansowanych ze środków publicznych (moduł o nazwie „Twój Portal"), wykazu miejsc, w których udzielana jest pomoc medyczna w ramach powszechnego ubezpieczenia zdrowotnego z podziałem na rodzaje udzielanych świadczeń oraz realizowane są recepty refundowane przez NFZ (moduł o nazwie „Gdzie się leczyć?"). Ponadto ma możliwość sprawdzenia swojego stanu ubezpieczenia (moduł o nazwie „Prawo do świadczeń), a także ma dostęp do modułu ustawień systemowych, gdzie może m.in. dokonać zmiany hasła oraz zmiany adresu e-mail. Moduły o nazwach „Twój portal" i „Gdzie się leczyć" są modułami dostępnymi bez konieczności logowania z uwagi na to, że nie umożliwiają one dostępu do danych osobowych. Za pośrednictwem systemu ZIP pacjent ma również możliwość zgłaszania nieprawidłowości związanych z udzielonymi mu świadczeniami opieki zdrowotnej. W zgłoszeniu takiej nieprawidłowości użytkownik obowiązkowo podaje rodzaj nieprawidłowości (nie udzielono świadczenia / sam zapłacił za to

zdrowotnego oraz numerach NIP i REGON płatnika ubezpieczenia zdrowotnego - na podstawie informacji przetwarzanych w Centralnym Wykazie Ubezpieczonych; 2) udzielonych mu świadczeniach opieki zdrowotnej oraz kwocie środków publicznych wydatkowanych na sfinansowanie tych świadczeń. Art. 192a. W celu potwierdzenia udzielenia świadczeń opieki zdrowotnej, Fundusz może zwrócić się do świadczeniobiorcy o informację w zakresie udzielonych mu świadczeń opieki zdrowotnej.

świadczenie i posiada dowód zapłaty / sam zapłacił za to świadczenie, ale nie posiada dowodu zapłaty / inna przyczyna). Opcjonalnie w zgłoszeniu użytkownik może podać imię i nazwisko oraz numer telefonu lub adres korespondencyjny. Informacje wprowadzone przez użytkownika w trakcie zgłaszania nieprawidłowości nie są zapisywane w systemie ZIP. Zgłoszenie nieprawidłowości nie jest drogą elektroniczną wysyłane do NFZ, użytkownik może je natomiast wydrukować i po podpisaniu wysłać pocztą lub zanieść osobiście do dowolnego oddziału wojewódzkiego NFZ (na wydruku zgłoszenia, oprócz informacji wprowadzonych przez użytkownika, znajdują się informacje pozwalające zidentyfikować kwestionowane świadczenie i oddział wojewódzki NFZ, które je sfinansował). Po otrzymaniu zgłoszenia NFZ rozpoczyna procedurę kontrolną mającą na celu wyjaśnienie okoliczności sprawy.

Istotne były również ustalenia poczynione w toku kontroli przeprowadzonej w jednym z podmiotów leczniczych[35] wykonującym działalność leczniczą m.in. w zakresie neurologii, neurochirurgii i psychiatrii, które wykazały, że były pracownik (lekarz) zgubił bloczki wypełnionych zaświadczeń lekarskich ZUS ZLA opatrzonych pieczęcią ww. podmiotu leczniczego. Kontrola wykazała, iż do dnia pozyskania przez kierownika podmiotu leczniczego informacji o tym, że do takiego zdarzenia doszło, mając na względzie art. 58 ust. 1 pkt 3 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 2010 r. Nr 77, poz. 512 z późn. zm.)[36] nie nadzorowano sposobu zabezpieczania przez lekarzy zaświadczeń lekarskich ZUS ZLA, ponieważ obowiązek ich zabezpieczenia spoczywał na lekarzach je wystawiających. Uznano bowiem, że to lekarze bezpośrednio pobierają z Zakładu Ubezpieczeń Społecznych druki zaświadczeń lekarskich ZUS ZLA i zobowiązani są do ich zabezpieczenia. Jednakże w związku z zaistniałym zdarzeniem kontrolowany podmiot leczniczy niezwłocznie po uzyskaniu informacji o tym zdarzeniu podjął działania w celu wyjaśnienia zaistniałej sytuacji i wykluczenia podobnych zdarzeń w przyszłości. Następnie zarządzeniem kierownika podmiotu leczniczego wdrożona została procedura dotyczącą zabezpieczania zaświadczeń lekarskich ZUS ZLA. Zgodnie z powołaną procedurą, wszyscy lekarze zatrudnieni w kontrolowanym podmiocie wystawiający pacjentom zaświadczenia ZUS ZLA zobowiązani

[35] Kontrola DIS-K-421/56/13

[36] Art. 58 ust. 1 pkt 3 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa. Zaświadczenie lekarskie wystawia się z dwiema kopiami, drugą kopię wystawiający zaświadczenie przechowuje przez okres 3 lat.

zostali do przeznaczenia odrębnego bloczka tych zaświadczeń wyłącznie dla pacjentów tego podmiotu. Procedura określiła również sposób postępowania z wypełnionymi zaświadczeniami oraz zasady ich przechowywania. Jak ustalono, podstawą wdrożenia powołanej procedury było stanowisko Generalnego Inspektora Ochrony Danych Osobowych wyrażone w decyzji z dnia 6 marca 2012 r. o sygn. DIS/DEC-174/12/14274. Biorąc pod uwagę działania podjęte przez kontrolowany podmiot leczniczy oraz prowadzenie przez właściwą prokuraturę postępowania w sprawie zagubienia przez byłego lekarza tegoż podmiotu bloczków wypełnionych zaświadczeń lekarskich ZUS ZLA, niecelowe było kierowanie przez Generalnego Inspektora żądania wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień, zgodnie z art. 17 ust. 2 ustawy o ochronie danych osobowych[37].

Do ciekawych należała kontrola przeprowadzona w jednej ze spółek[38] prowadzącej serwis internetowy, w ramach którego oferuje użytkownikom, tj. osobom fizycznym, zarejestrowanym w serwisie i posiadającym konto użytkownika, możliwość korzystania z płatnych usług obejmujących konsultacje medyczne online oraz konsultacje okołomedyczne online. W ramach konsultacji medycznych online, ww. spółka umożliwia zarejestrowanym użytkownikom serwisu, po uprzednim wniesieniu opłaty za usługę, zadawanie pytań zatrudnionym w spółce lekarzom. Usługa konsultacji medycznych dostępna jest za pośrednictwem systemu wideokonsultacji. W toku kontroli wyjaśniono, że usługa ta polega na świadczeniu edukacji zdrowotnej za pośrednictwem systemu wideokonsultacji i obejmuje: przeprowadzenie analizy dokumentacji medycznej przedstawionej przez użytkownika serwisu celem udzielenia konsultacji medycznej, edukowanie i informowanie o możliwości przyjmowania określonych leków, które można nabyć bez recepty, jak również o lekach, które, po zbadaniu pacjenta przez lekarza, uzyskuje się na receptę, edukowanie i informowanie o możliwych działaniach niepożądanych w zażywaniu lekarstw i innych środków farmakologicznych, informowanie o potrzebie wykonania badań laboratoryjnych lub potrzebie poddania się badaniu lekarskiemu, kierowanie użytkownika serwisu na wizytę lekarską lub badania diagnostyczne do współpracującej ze spółką placówki udzielającej

[37] Art. 17 ust. 2. Na podstawie ustaleń kontroli inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.
[38] Kontrola DIS-K-421/169/12

świadczeń zdrowotnych, w przypadku gdy użytkownik wyrazi taką wolę. W ramach usług konsultacji okołomedycznych online spółka oferuje użytkownikom serwisu konsultacje za pośrednictwem systemu wideokonsultacji z osobami niebędącymi lekarzami, a wykonującymi zawód związany z ochroną zdrowia, w tym m.in. z zakresu specjalizacji pielęgniarskiej i położniczej.

W toku kontroli ustalono, że spółka nie była wpisana do rejestru podmiotów wykonujących działalność leczniczą, prowadzonego przez właściwego wojewodę. W ocenie spółki, świadczone przez nią usługi w zakresie konsultacji medycznych i okołomedycznych online były wyłącznie usługami edukacji zdrowotnej prowadzonej za pośrednictwem serwisu internetowego i nie stanowią świadczeń zdrowotnych w rozumieniu ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2013 r. poz. 217). Ustalono ponadto, że spółka ta przetwarzała m.in. dane osobowe użytkowników serwisu, tj. osób fizycznych, które dokonały rejestracji w serwisie i posiadały konto użytkownika. Dane te były przetwarzane w zbiorze danych zgłoszonym przez spółkę do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Dane do zbioru były pozyskiwane wyłącznie od osób, których dotyczą, za pomocą formularza rejestracyjnego dostępnego na stronie internetowej serwisu. Zakres danych przetwarzanych w zbiorze obejmował: imię, nazwisko, datę urodzenia, numer PESEL, adres zamieszkania, numer telefonu, adres e-mail, płeć. Ponadto w przedmiotowym zbiorze spółka przetwarzała informacje dotyczące stanu zdrowia użytkowników serwisu ujawnione przez nich podczas konsultacji medycznych online i konsultacji okołomedycznych online w związku z tym, że przebieg tych konsultacji był utrwalany za pomocą urządzeń rejestrujących obraz i dźwięk.

Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące prawo[39] Generalny Inspektor Ochrony Danych Osobowych uznał, iż przetwarzanie przez spółkę

[39] 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. 2 ust. 1 pkt 10 ustawy o działalności leczniczej (Dz. U. z 2013 r. poz. 217). Świadczeniem zdrowotnym są działania służące zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania. Art. 2 ust. 1 pkt 2 ww. ustawy, osobą wykonującą zawód medyczny jest osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoba legitymująca się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny. Art. 2 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2011 r. Nr 277, poz. 1634 z późn. zm.), wykonywanie zawodu lekarza polega na udzielaniu przez osobę posiadającą wymagane kwalifikacje, potwierdzone odpowiednimi dokumentami, świadczeń zdrowotnych, w szczególności: badaniu

danych osobowych osób korzystających ze świadczonych przez ten podmiot w ramach serwisu internetowego usług konsultacji medycznych i okołomedycznych, udzielanych przez lekarzy, pielęgniarki i położne, odbywało się niezgodnie z prawem z uwagi na to, iż w świetle obowiązujących przepisów usługi te stanowią świadczenia zdrowotne w rozumieniu art. 2 ust. 1 pkt 10 ustawy o działalności leczniczej. W związku z tym spółka, nie posiadając wpisu do rejestru podmiotów wykonujących działalność leczniczą prowadzonego przez właściwego wojewodę, nie była uprawniona do prowadzenia działalności w zakresie świadczenia ww. usług, a tym samym do przetwarzania danych osób korzystających z tych usług. Działanie podmiotu kontrolowanego naruszało zatem art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych, ze względu na przetwarzanie danych osobowych niezgodnie z prawem.

W toku kontroli ustalono także, że w ramach usług konsultacji okołomedycznych online spółka oferowała zarejestrowanym użytkownikom serwisu, obok konsultacji z zakresu specjalizacji pielęgniarskiej i położniczej, również konsultacje z zakresu specjalizacji psychologicznej, dietetycznej oraz fizjoterapeutycznej. Usługi te w imieniu spółki świadczyły zatrudnione w spółce osoby posiadające stosowne kwalifikacje (psychoterapeuci, dietetycy oraz fizjoterapeuci). Ujawnione podczas konsultacji okołomedycznych dane o stanie zdrowia

---

stanu zdrowia, rozpoznawaniu chorób i zapobieganiu im, leczeniu i rehabilitacji chorych, udzielaniu porad lekarskich, a także wydawaniu opinii i orzeczeń lekarskich. Art. 4 ust. 1 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2011 r. Nr 174, poz. 1039 z późn. zm.), wykonywanie zawodu pielęgniarki polega na udzielaniu świadczeń zdrowotnych, w szczególności na: rozpoznawaniu warunków i potrzeb zdrowotnych pacjenta; rozpoznawaniu problemów pielęgnacyjnych pacjenta; planowaniu i sprawowaniu opieki pielęgnacyjnej nad pacjentem; samodzielnym udzielaniu w określonym zakresie świadczeń zapobiegawczych, diagnostycznych, leczniczych i rehabilitacyjnych oraz medycznych czynności ratunkowych; realizacji zleceń lekarskich w procesie diagnostyki, leczenia i rehabilitacji; orzekaniu o rodzaju i zakresie świadczeń opiekuńczo-pielęgnacyjnych; edukacji zdrowotnej i promocji zdrowia. Art. 5 ust. 1 ww. ustawy, wykonywanie zawodu położnej polega na udzielaniu świadczeń zdrowotnych. Art. 5 ust. 1 ustawy o działalności leczniczej, lekarze i pielęgniarki (położne) mogą wykonywać swój zawód w ramach działalności leczniczej na zasadach określonych w ustawie oraz w przepisach odrębnych, po wpisaniu do rejestru podmiotów wykonujących działalność leczniczą, o którym mowa w art. 100. Art. 3 ust. 1 przedmiotowej ustawy, działalność lecznicza polega na udzielaniu świadczeń zdrowotnych. Działalność lecznicza może również polegać na: 1) promocji zdrowia lub 2) realizacji zadań dydaktycznych i badawczych w powiązaniu z udzielaniem świadczeń zdrowotnych i promocją zdrowia, w tym wdrażaniem nowych technologii medycznych oraz metod leczenia (art. 3 ust. 2). Art. 16 ust. 1 ustawy o działalności leczniczej, działalność lecznicza jest działalnością regulowaną w rozumieniu ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2013 r. poz. 672 z późn. zm.). Art. 64 ust. 1 ustawy o swobodzie działalności gospodarczej. Jeżeli przepis odrębnej ustawy stanowi, że dany rodzaj działalności jest działalnością regulowaną w rozumieniu ustawy o swobodzie działalności gospodarczej, przedsiębiorca może wykonywać tę działalność, jeżeli spełnia szczególne warunki określone przepisami tej odrębnej ustawy i po uzyskaniu wpisu w rejestrze działalności regulowanej, z zastrzeżeniem art. 75. Art. 103 ustawy o działalności leczniczej, działalność leczniczą można rozpocząć po uzyskaniu wpisu do rejestru podmiotów wykonujących działalność leczniczą, z zastrzeżeniem art. 104. Organem prowadzącym rejestr jest wojewoda właściwy dla siedziby albo miejsca zamieszkania podmiotu leczniczego – w odniesieniu do podmiotów leczniczych (art. 106 ust. 1).

(przebieg konsultacji był utrwalany przez spółkę za pomocą urządzeń rejestrujących obraz i dźwięk) były przetwarzane w zbiorze danych, który został zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. W toku kontroli wyjaśniono, że podstawą prawną przetwarzania przez spółkę danych osobowych użytkowników serwisu korzystających ze świadczonych przez spółkę usług, dotyczących stanu zdrowia ujawnionych podczas konsultacji okołomedycznych online, jest art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych[40].

Oceniając powyższy stan faktyczny Generalny Inspektor Ochrony Danych Osobowych wskazał, iż przesłanka przetwarzania danych osobowych określona w art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych ma zastosowanie wyłącznie w przypadku przetwarzania danych osobowych przez podmioty, bądź osoby zawodowo trudniące się leczeniem lub świadczeniem innych usług medycznych w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów oraz zarządzania udzielaniem usług medycznych. Natomiast w związku z tym, że spółka nie jest podmiotem leczniczym w rozumieniu ustawy o działalności leczniczej i nie jest również podmiotem zajmującym się zarządzaniem udzielaniem usług medycznych, nie może skutecznie powoływać się na ww. przesłankę przetwarzania danych osobowych. Ponadto w toku kontroli ustalono, że osoby, których dane dotyczą, nie wyrażały zgody na piśmie na przetwarzanie przez spółkę ich danych osobowych ujawnionych w toku konsultacji okołomedycznych online. Spółka nie legitymuje się też żadną z pozostałych przesłanek wskazanych w art. 27 ust. 2 ustawy o ochronie danych osobowych[41] legalizujących przetwarzanie danych osobowych szczególnie

[40] Art. 27 ust. 2 pkt 7 ustawy. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych.

[41] Art. 27 ust. 1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Art. 27 ust. 2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli: 1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych, 2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony, 3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora, 4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością

chronionych. W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych uznał, że przetwarzanie przez spółkę danych osobowych użytkowników serwisu, dotyczących stanu zdrowia, w związku ze świadczeniem usług konsultacji okołomedycznych online z zakresu specjalizacji psychologicznej, dietetycznej oraz fizjoterapeutycznej, odbywa się bez podstawy prawnej.

Z uwagi na stwierdzone uchybienia w procesie przetwarzania danych osobowych, wobec spółki zostało wszczęte postępowanie administracyjne. W toku postępowania spółka usunęła ww. uchybienia stanowiące przedmiot postępowania. Z powyższych względów postępowanie w tym zakresie zostało umorzone.

Mając na uwadze dokonane w toku kontroli ustalenia, z których wynikało, że świadczone przez spółkę usługi konsultacji medycznych w ramach serwisu są udzielane przez zatrudnionych w spółce lekarzy za pośrednictwem systemu wideokonsultacji, tj. na odległość, oraz biorąc pod uwagę obowiązujące przepisy dotyczące wykonywania zawodu lekarza, a w szczególności art. 2 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2011 r. Nr 277, poz. 1634 z późn. zm.) oraz art. 42 ww. ustawy[42], z których wynika, że orzekanie o stanie zdrowia określonej osoby, co do zasady powinno następować po uprzednim, osobistym jej zbadaniu przez lekarza, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Prezesa Naczelnej Rady Lekarskiej o objęcie przedmiotowej sprawy nadzorem przez organy samorządu zawodowego lekarzy.

---

i zapewnione są pełne gwarancje ochrony przetwarzanych danych, 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem, 6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie, 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych, 8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą, 9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone, 10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

[42] Art. 2 ust. 1 ustawy o zawodach lekarza i lekarza dentysty. Wykonywanie zawodu lekarza polega na udzielaniu przez osobę posiadającą wymagane kwalifikacje, potwierdzone odpowiednimi dokumentami, świadczeń zdrowotnych, w szczególności: badaniu stanu zdrowia, rozpoznawaniu chorób i zapobieganiu im, leczeniu i rehabilitacji chorych, udzielaniu porad lekarskich, a także wydawaniu opinii i orzeczeń lekarskich. Art. 42 ustawy o zawodach lekarza i lekarza dentysty. Lekarz orzeka o stanie zdrowia określonej osoby po uprzednim, osobistym jej zbadaniu, z zastrzeżeniem sytuacji określonych w odrębnych przepisach.

2.2.4. Oświata

W 2013 r. w placówkach oświatowych przeprowadzonych zostało **5 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Jedna z takich kontroli została przeprowadzona w spółce prowadzącej zajęcia pozalekcyjne (kursy wiedzy) dla dzieci i młodzieży ze szkół podstawowych (klasy od 4 do 6) i gimnazjów[43]. Spółka pozyskiwała za pomocą ankiet dane osobowe uczniów, które potem zostały zniszczone. W toku kontroli wskazano, iż podstawą prawną przetwarzania danych osobowych uczniów na wypełnionych przez nich ankietach był art. 23 ust. 1 pkt 1 ustawy, tj. ustna zgoda uczniów. Z uwagi na fakt, że uczniowie ww. szkoły nie mieli pełnej zdolności do czynności prawnych w rozumieniu przepisów prawa cywilnego (a zatem oświadczenie woli o wyrażeniu zgody było nieskuteczne), to należało uznać, iż spółka pozyskała dane osobowe uczniów bez podstawy prawnej. W takim przypadku przetwarzanie danych uczniów odbywałoby się zgodnie z przepisami prawa, gdyby zgodę wyrazili ich przedstawiciele ustawowi. Jednakże z uwagi na to, iż ankiety stosowane przez spółkę zostały zniszczone, a tym samym usunięto dane osobowe uczniów, niecelowe było wszczęcie postępowania administracyjnego w tym zakresie.

2.2.5. Telekomunikacja

W okresie sprawozdawczym u dostawców usług telekomunikacyjnych przeprowadzonych zostało **14 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych[44]. Sześć z nich zostało przeprowadzonych w związku z otrzymanymi przez Generalnego Inspektora zawiadomieniami o naruszeniu danych osobowych, złożonymi w trybie wynikającym z art. 174a ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)[45].

Jedna z tych kontroli[46] wykazała, iż podmiot kontrolowany prowadzi rejestr naruszeń danych osobowych na rzecz innego dostawcy publicznie dostępnych usług

[43] Kontrola DIS-K-421/127/13
[44] Np. kontrole DIS-K-421/13/13, DIS-K-421/110/13 i DIS-K-421/153/13.
[45] Art. 174a ust. 1. Dostawca publicznie dostępnych usług telekomunikacyjnych zawiadamia Generalnego Inspektora Ochrony Danych Osobowych o naruszeniu danych osobowych niezwłocznie, nie później niż w terminie 3 dni od stwierdzenia naruszenia.
[46] Kontrola DIS-K-421/114/13

telekomunikacyjnych bez podstawy prawnej, tj. bez umowy powierzenia, o której mowa w art. 31 ust. 1 ustawy o ochronie danych osobowych[47], a tym samym narusza art. 174d ust. 2 ustawy Prawo telekomunikacyjne[48]. W związku ze stwierdzonym uchybieniem w procesie przetwarzania danych osobowych zostało wszczęte postępowanie administracyjne, w toku którego podmiot kontrolowany usunął uchybienie i z tego względu postępowanie zostało umorzone.

Kolejna kontrola[49] związana z zawiadomieniem o naruszeniu danych osobowych, które zostało zgłoszone Generalnemu Inspektorowi przez dostawcę publicznie dostępnych usług telekomunikacyjnych na podstawie art. 174a ust. 1 ustawy Prawo telekomunikacyjne, dotyczyła omyłkowo skierowanej do jednego z abonamentów korespondencji dotyczącej innego abonenta. Naruszenie to powstało na skutek błędu pracownika podmiotu, któremu jednostka kontrolowana powierzyła przetwarzanie danych osobowych na podstawie z art. 31 ust. 1 ustawy o ochronie danych osobowych w zakresie wydruku, personalizacji i kopertowania korespondencji masowej celem jej dostarczania do abonentów. W wyniku przeprowadzonych czynności kontrolnych stwierdzono, iż nie doszło do naruszenia przepisów o ochronie danych osobowych, które mogłoby skutkować wszczęciem wobec dostawcy usług telekomunikacyjnych postępowania administracyjnego. Niemniej jednak, w celu zapobiegania w przyszłości podobnym naruszeniom, podmiot kontrolowany podjął działania zmierzające do określenia w drodze umowy zakresu odpowiedzialności oraz kar umownych za naruszenie przepisów ustawy o ochronie danych osobowych dotyczących zabezpieczenia danych abonentów.

Ponadto przeprowadzone zostały kontrole[50] u czterech dostawców publicznie dostępnych usług telekomunikacyjnych w związku z dokonanymi przez nich zawiadomieniami o naruszeniu danych osobowych związanego z tym samym incydentem. Incydent ten polegał na opublikowaniu w Internecie przez nieznaną osobę/osoby pliku zawierającego dane osobowe abonentów tych podmiotów (405833 rekordów zawierających dane osobowe).

[47] Art. 31 ust. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
[48] Art. 174d ust. 2. Dostawca publicznie dostępnych usług telekomunikacyjnych może powierzyć, w drodze umowy, innemu przedsiębiorcy prowadzenie rejestru naruszeń danych osobowych.
[49] Kontrola DIS-K-421/113/1
[50] Np. kontrole DIS-K-421/170/13 i DIS-K-421/173/13.

2.2.6. Zatrudnienie

Jedną z ciekawszych kontroli przeprowadzonych w 2013 r. dotyczących zagadnień z zakresu zatrudnienia była kontrola przeprowadzona w związku ze skargą związku zawodowego działającego w jednej ze spółek[51]. Skarga dotyczyła przetwarzania danych osobowych pracowników pozyskiwanych w ramach wprowadzonej w spółce procedury mającej na celu wyłonienie spośród pracowników aktualnie zajmujących stanowiska dziennikarskie, kandydatów na dwa rodzaje stanowisk, tj. do pełnienia funkcji koordynacyjno-programowej i funkcji koordynacyjno-realizacyjnej. Ustalono, iż wynikiem przeprowadzonej procedury miały być promocje (awanse) udzielone na podstawie decyzji komisji ewaluacyjnych, wskazujące osoby przewidziane do pełnienia zadań przypisanych każdej ze ww. funkcji. Przystąpienie do procedury było dobrowolne. O jej wdrożeniu pracownicy zostali poinformowani drogą elektroniczną oraz w formie biuletynu. Przystąpienie do procedury nie miało charakteru sformalizowanego i następowało poprzez udział w sesji testowej. Przedmiotowa procedura miała charakter wielostopniowy. W pierwszym etapie kwalifikacje pracowników były oceniane na podstawie kwestionariusza ewaluacyjnego przez członków komisji ewaluacyjnej, w skład której wchodzili dyrektorzy poszczególnych jednostek organizacyjnych lub osoby wskazane przez dyrektorów, oraz bezpośredni przełożony danego pracownika. Drugim etapem procedury była testowa ocena predyspozycji pracowników rozpoczynająca się od wprowadzenia pracowników, którzy przyszli na sesję, w przebieg procedury, jej zasady i cele oraz techniczne informacje na temat przeprowadzenia testów. Pracownicy byli także informowani o dobrowolności przystąpienia do procedury i możliwości dostępu do przeprowadzonych testów i ich wyników. Po przekazaniu ww. informacji pracownicy, którzy pozostali na sesji, wypełniali w formie papierowej trzy testy: kwestionariusz sytuacyjny, który obrazował sytuację pracy koordynatora, wielowymiarowy kwestionariusz preferencji i test inwentarz motywacji osiągnięć. Za ten etap procedury odpowiadali pracownicy spółki posiadający wykształcenie psychologiczne. Trzecim etapem procedury były rozmowy indywidualne z pracownikami poddanymi testom przeprowadzane przez komisję ewaluacyjną, w skład której wchodzili: dyrektorzy poszczególnych jednostek organizacyjnych lub osoby wskazane przez dyrektorów, bezpośredni przełożony danego pracownika oraz pracownicy działu rekrutacji

[51] Kontrola DIS-K-421/144/13

kontrolowanego podmiotu. Rozmowy polegały na wywiadzie dotyczącym doświadczeń zawodowych, „obronie" kwestionariusza sytuacyjnego i pytaniach sytuacyjnych.

Zakres danych pracowników, którzy wzięli udział w procedurze, pozyskiwany za pomocą wielowymiarowego kwestionariusza preferencji oraz testu inwentarz motywacji osiągnięć, obejmował m.in.: imię, nazwisko, płeć, wiek, wykształcenie, zawód wyuczony, zawód wykonywany, miejsce zamieszkania, zainteresowania językowe, preferencje w zakresie planowania-improwizacji, dane dotyczące skal np. elastyczność, odwaga, preferowanie trudnych zadań, dominacja, ukierunkowanie na cel, zaangażowanie, internalizacja, wytrwałość, samokontrola.

Zakres danych pozyskiwany za pomocą kwestionariuszy sytuacyjnych dotyczył m.in.: umiejętności rozwiązywania problemów, ustalania priorytetów, organizowania pracy pod presją, rozwiązywania sytuacji konfliktowych, samodzielności i inicjatywy. Za pomocą kwestionariuszy oceny kompetencji pozyskiwano informacje dotyczące: warsztatu dziennikarskiego, znajomości regulacji wewnętrznych w zakresie programowania, przygotowania i produkcji audycji, znajomości technologii produkcji audycji telewizyjnych, umiejętności dokumentacyjne, samodzielności i inicjatywy, rozwiązywania sytuacji konfliktowych, elastyczności, wszechstronności i otwartości na nowe doświadczenia, ustalania priorytetów, inicjatywy w rozwiązywaniu problemów, umiejętności organizacyjnych, postawy zgodnej z zasadami etyki dziennikarskiej, kwalifikacji merytorycznych, umiejętności interpersonalnych i społecznych, umiejętności koordynacji zadań oraz standardów etyki dziennikarskiej.

Jak wyjaśniono w toku kontroli, celem przetwarzania przedmiotowych danych osobowych pracowników było nawiązanie stosunku pracy. Szczegółowy cel przetwarzania danych stanowiło wyłonienie pracowników, którzy otrzymają awans na stanowiska kluczowe z punktu widzenia interesów pracodawcy.

Po przeprowadzeniu ww. kontroli podmiot kontrolowany poinformował Generalnego Inspektora, iż usunięto dane osobowe jego pracowników zebrane za pomocą testów psychometrycznych (w formie papierowej i elektronicznej). Dlatego też Generalny Inspektor uznał, iż z analizy kwestionariuszy sytuacyjnych oraz kwestionariuszy oceny kompetencji wynika, iż zakres danych osobowych dotyczących pracowników, będących jednocześnie kandydatami do pracy aplikującymi na stanowiska koordynacyjne opisane w przedmiotowej

procedurze, nie wykracza poza zakres wskazany w art. 22^1 ustawy Kodeks pracy[52], a zatem nie zostały naruszone przepisy o ochronie danych osobowych.

2.2.7. Internet

W okresie sprawozdawczym w podmiotach prowadzących serwisy internetowe, w tym sklepy internetowe, przeprowadzonych zostało **10 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

W toku jednej z takich kontroli[53] stwierdzono, że wśród danych pozyskiwanych od użytkowników portalu były m.in. numer PESEL oraz informacja o niepełnosprawności. Kontrola wykazała, iż przedsiębiorca pozyskuje od użytkowników portalu internetowego, którzy nie dokonali w sklepie internetowym tego portalu zakupu produktu podlegającego refundacji przez Narodowy Fundusz Zdrowia, dane osobowe w zakresie numeru PESEL, w celu ewentualnego wykorzystania w przypadku, gdyby użytkownik dokonał zakupu. Generalny Inspektor uznał, iż skoro informacja dotycząca numeru PESEL była pozyskiwana na wypadek, gdyby użytkownik dokonał ww. zakupu - co może nigdy nie nastąpić – to należy uznać, iż jest zbierana niejako „na zapas", co narusza zasadę związania celem, o której mowa w art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych[54]. Informacja o niepełnosprawności była zaś pozyskiwana od użytkowników, o których mowa powyżej, bez zgody tych osób wyrażonej na piśmie, a więc administrator danych nie legitymował się podstawą prawną przetwarzania danych tych osób wynikającą z art. 27 ust. 2 pkt 1 ustawy

[52] Art. 22^1 § 1. Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko, 2) imiona rodziców, 3) datę urodzenia, 4) miejsce zamieszkania (adres do korespondencji), 5) wykształcenie, 6) przebieg dotychczasowego zatrudnienia. § 2. Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także: 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, 2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL). § 3. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 2. § 4. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. § 5. W zakresie nieuregulowanym w § 1-4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

[53] Kontrola DIS-K-421/46/13

[54] 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 zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

o ochronie danych osobowych[55]. W związku ze stwierdzonymi u przedsiębiorcy uchybieniami w procesie przetwarzania danych osobowych, zostało wszczęte postępowanie administracyjne. W toku prowadzonego postępowania przedsiębiorca usunął ww. uchybienia i z tego względu postępowanie zostało umorzone.

2.2.8. RFID

W okresie sprawozdawczym przeprowadzono **8 kontroli**[56] w podmiotach przetwarzających dane osobowe w związku z wykorzystaniem technologii automatycznej identyfikacji radiowej (Radio Frequency Identification - RFID). Technologia ta znajduje zastosowanie w coraz to nowych obszarach życia człowieka. Ochrona danych jest kluczowym problemem rozwoju tej technologii. W dniu 12 maja 2009 r. Komisja Europejska wydała zalecenie w sprawie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową[57]. We wspomnianym zaleceniu poproszono państwa członkowskie, aby zapewniły „opracowanie przez sektor we współpracy z odpowiednimi zainteresowanymi stronami (…) ram do oceny skutków w zakresie ochrony danych i prywatności”.[58] Jeden z głównych problemów w zakresie ochrony prywatności, związanych ze ww. technologią, „wiąże się z wykorzystywaniem technologii RFID, które obejmują śledzenie osób i uzyskiwanie dostępu do danych osobowych”. Chociaż operator RFID, wprowadzając zastosowanie RFID, może nie kierować się tym celem, należy wziąć pod uwagę ryzyko, że osoba trzecia może wykorzystać identyfikatory do takich niezamierzonych celów. Zmienione ramy wyraźnie wymagają od operatorów RFID dokonania oceny ryzyka, jakie może wiązać się z wykorzystaniem identyfikatorów poza granicami zastosowania RFID lub noszeniem ich przez osoby fizyczne. Na problem ten zwrócił szczególną uwagę sektor detaliczny, którego przedstawiciele obawiają się, że przedmioty z identyfikatorem kupowane przez osoby fizyczne mogłyby być niewłaściwie wykorzystane przez detalistów lub osoby trzecie

[55] Art. 27 ust. 2 pkt 1. Przetwarzanie 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, jest dopuszczalne, jeżeli osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych.
[56] Np. kontrole DIS-K-421/8/13, DIS-K-421/22/13 i DIS-K-421/25/13.
[57] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[58] Opinia 9/2011 na temat zmienionej propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID, przyjęta w dniu 11 lutego 2011 r.

do celów śledzenia lub opracowywania profili. Komisja Europejska zajęła się tym problemem w wydanym przez siebie zaleceniu, ustalając zasadę, zgodnie z którą identyfikatory muszą być dezaktywowane w punkcie sprzedaży, chyba że konsumenci wyrażą świadomą zgodę na dalsze ich działanie. W tym samym zaleceniu zezwala się na wyjątek od wspomnianej zasady dezaktywacji w przypadku, gdy ocena skutków w zakresie ochrony danych osobowych i prywatności wykaże, że dalsze działanie identyfikatorów po opuszczeniu punktu sprzedaży nie wiąże się z „prawdopodobieństwem zagrożenia dla prywatności lub ochrony danych osobowych”[59].

Przedstawione powyżej zagadnienia, na które uwagę zwróciła już Komisja Europejska, tylko częściowo znalazły odzwierciedlenie w materiale z przeprowadzonych kontroli. Przede wszystkim nie stwierdzono, aby ta technologia była wykorzystywana do przetwarzania danych osobowych klientów w sektorze handlu detalicznego. Technologia RFID jest powszechnie wykorzystywana natomiast w celu kontroli dostępu do pomieszczeń. Jej zastosowanie łączy się w głównej mierze z przetwarzaniem danych osobowych pracowników korzystających z pomieszczeń objętych systemem kontroli dostępu.

Na podstawie dokonanych w toku kontroli ustaleń stwierdzono, że poddane kontrolom podmioty wykorzystywały wskazaną technologię głównie do przetwarzania danych osobowych pracowników (kontrola dostępu i kontrola czasu pracy) i w tym zakresie nie stwierdzono większych zagrożeń dla przetwarzania danych osobowych przy jej użyciu. Tylko jedna kontrola wykazała, że technologia była wykorzystywana do przetwarzania danych osobowych klientów, ale i w tym przypadku nie stwierdzono, aby wiązała się ona z większym niebezpieczeństwem w obszarze przetwarzania danych osobowych tych osób. Natomiast stwierdzone uchybienia dotyczyły głównie systemów informatycznych i polegały na naruszeniu następujących obowiązków wynikających z przepisów o ochronie danych osobowych: przetwarzaniu danych osobowych po osiągnięciu celu przetwarzania tych danych, niedopełnieniu wymogu zmiany hasła nie rzadziej niż co 30 dni, braku zapewnienia przez system służący do przetwarzania danych osobowych odnotowania daty pierwszego wprowadzenia danych do tego systemu lub/oraz identyfikatora użytkownika wprowadzającego te dane, a także braku zapewnienia dla każdej osoby, której dane osobowe

[59] Zob. na przykład Opinia 5/2010 (WP 175) i WP 105 „Dokument roboczy na temat kwestii zakresu ochrony danych związanych z technologią RFID”, 19 stycznia 2005 r.

są przetwarzane w systemie informatycznym, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie ww. informacje.

Na podstawie stwierdzonych w toku kontroli uchybień w procesie przetwarzania danych osobowych wobec podmiotów, które dopuściły do naruszenia przepisów o ochronie danych osobowych zostały wszczęte postępowania administracyjne. Z uwagi jednak na usunięcie nieprawidłowości przez jednostki kontrolowane w toku postępowania administracyjnego Generalny Inspektor wydał decyzje umarzające postępowania[60].

2.2.9. Programy lojalnościowe

W okresie sprawozdawczym w podmiotach prowadzących programy lojalnościowe zostało przeprowadzonych **7 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych[61].

W ramach programów lojalnościowych funkcjonują programy oszczędnościowe polegające na używaniu podczas zakupów specjalnych kart przypisanych do indywidualnych kont, na których gromadzone są środki, umożliwiające uzyskanie rabatu przy kolejnych zakupach lub oszczędzanie poprzez zbieranie punktów podczas dokonywania zakupów. Niektóre programy lojalnościowe nagradzają uczestników punktami, które mogą następnie podlegać wymianie na kupony rabatowe lub nagrody. Jak ustalono, większość objętych kontrolami podmiotów oferowała klientom program prowadzony samodzielnie lub we współpracy z podwykonawcami. Część programów była też prowadzona wspólnie z innymi podmiotami, np. bankami i instytucjami finansowymi. Programy te wiązały się z możliwością skorzystania przez klienta zarówno z produktów finansowych np. kart przedpłaconych lub kredytowych, jak i z programu lojalnościowego. Jeden z badanych podmiotów oferował swoim klientom możliwość skorzystania z programu lojalnościowego prowadzonego przez podmiot zewnętrzny, z którym zawarł umowę współpracy w tym zakresie[62]. Zasady funkcjonowania poszczególnych programów określają dostępne dla klientów regulaminy, z którymi zapoznanie jest warunkiem przystąpienia do programów.

[60] Np. decyzje DIS/DEC-630/13/37898 i DIS/DEC-731/13/44150.
[61] Np. kontrole DIS-K-421/25/13, DIS-K-421/30/13 i DIS-K-421/36/13.
[62] Kontrola DIS-K-421/32/13

W przeważającej większości przypadków jako podstawę prawną przetwarzania danych osobowych uczestników programów lojalnościowych podmioty objęte kontrolą podawały zgodę osób, których dane dotyczą, określoną w art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych. Tylko jeden z podmiotów wskazał, iż podstawą prawną przetwarzania danych osobowych uczestników programu jest art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych, tj. wykonanie umowy, jaką klient zawiera przystępując do programu lojalnościowego. Biorąc pod uwagę wyrażoną w art. 353^1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16 poz. 93 z późn. zm.)[63] zasadę swobody umów, należy stwierdzić, że *„(...) strony mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości stosunku, ustawie, zasadom współżycia społecznego*" (wyrok SA w Warszawie z dnia 26 stycznia 2006 r. VI ACa 841/2005, niepubl.). Zasada swobody umów jest pochodną konstytucyjnej zasady wolności gospodarczej (por. wyrok SN z dnia 4 października 2006 r. II CSK 117/2006, LEX nr 332959). Swoboda kształtowania treści umowy przy uwzględnieniu brzmienia art. 353^1 K.c. oznacza, że strony mają możliwość zawarcia umowy nienazwanej, której treść ukształtują samodzielnie wedle swego uznania (będziemy mieli wówczas do czynienia ze swobodą kreowania stosunków umownych, nieobjętych katalogiem umów nazwanych) (wyrok SN z dnia 6 listopada 2002 r. I CKN 1144/00, LEX nr 74505). Artykuł 353^1 K.c. wprowadza trzy ograniczenia tej wolności: ustawę, właściwość (naturę) stosunku prawnego i zasady współżycia społecznego (por. np. wyrok SN z dnia 6 listopada 2003 r. I CKN 1144/2000, Monitor Prawniczy 2004, Nr 5, s. 233). Z powyższych względów, należy uznać że nie ma przeszkód, aby organizator programu lojalnościowego określił swoje relacje z uczestnikiem tego programu jako umowę, a tym samym powoływał się na przesłankę przetwarzania jego danych wskazaną w art. 23 ust. 1 pkt 3 ustawy.

Wątpliwości wzbudziła jednak stosowana w niektórych podmiotach konstrukcja oświadczeń o wyrażeniu zgody (klauzul). Uznano, iż może ona wprowadzać w błąd, bowiem wymaga od klienta działania (zaznaczenia pola) w sytuacji, kiedy nie zgadza się na wykorzystanie jego danych we wskazanych celach. Zatem może mieć miejsce sytuacja, gdy klient poprzez brak swojej aktywności (także brak wnikliwości przy czytaniu klauzul) wyrazi

[63] Art. 353^1. Strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego.

zgodę na przetwarzanie danych w określonych celach. Taki sposób sformułowania oświadczenia może pozostawać w sprzeczności z powinnością dołożenia przez administratora danych szczególnej staranności – o której mowa w art. 26 ust. 1 ustawy o ochronie danych osobowych – w celu ochrony interesów osób, których dane przetwarza.

Na podstawie dokonanych ustaleń stwierdzono, że skontrolowane podmioty oferujące programy lojalnościowe naruszają przepisy o ochronie danych osobowych w zakresie konstrukcji treści oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych, braku aktualizacji zgłoszenia zbioru danych osobowych do rejestracji Generalnemu Inspektorowi, a przede wszystkim zastosowanych środków technicznych i organizacyjnych mających na celu zabezpieczenie danych (polegających m.in. na braku zapewnienia przez system służący do przetwarzania danych osobowych odnotowania daty pierwszego wprowadzenia danych do tego systemu lub/oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu i niedopełnieniu obowiązku dotyczącego długości znaków w haśle oraz jego złożoności), a także w zakresie prowadzonej dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

W związku z uchybieniami stwierdzonymi w toku kontroli wydane zostały decyzje nakazujące usunięcie uchybień w procesie przetwarzania danych osobowych, a także decyzje umarzające postępowanie w zakresie nieprawidłowości usuniętych przez jednostki kontrolowane w toku postępowania[64]. W wydanych decyzjach Generalny Inspektor nakazał m.in. zapewnienie klientom przystępującym do programu lojalnościowego możliwości swobodnego wyrażenia oświadczenia woli, którego treścią jest zgoda na przetwarzanie danych osobowych, zastosowanie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia w systemie informatycznym oraz wobec danych wprowadzanych na stronie www w procesie rejestracji konta w systemie informatycznym, a także opracowanie w formie pisemnej dokumentacji stanowiącej politykę bezpieczeństwa.

2.2.10. Inne

Istotne problemy w procesie przetwarzania danych osobowych stwierdzone zostały również w toku kontroli przeprowadzonych w podmiotach nienależących do żadnego z przedstawionych wyżej sektorów.

[64] Np. DIS/DEC-628/13/37521, DIS/DEC-630/13/37898 i DIS/DEC-722/13/42803.

Kontrola jednej z organizacji pożytku publicznego[65] wykazała, że organizacja ta prowadziła zbiór danych osobowych w związku z zarządzaniem ośrodkami wypoczynkowymi, które świadczą usługi noclegowe i gastronomiczne. Ustalono, że w przedmiotowym zbiorze przetwarzane były dane osobowe gości przebywających w ww. ośrodkach, pozyskiwane w związku z koniecznością spełnienia obowiązku meldunkowego wynikającego z 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.) oraz w celu wystawienia faktury. Do książek meldunkowych wprowadzane były dane z dowodu osobistego tj.: imię i nazwisko, imiona rodziców, data i miejsce urodzenia, seria i numer dowodu osobistego, ponadto wpisywano datę przybycia do ośrodka i okres pobytu. Na podstawie ustalonego stanu faktycznego Generalny Inspektor wskazał, że brak jest aktualnie podstaw prawnych do przetwarzania danych osobowych gości ośrodków wypoczynkowych w celu dopełnienia obowiązku meldunkowego z uwagi na to, iż obowiązek ten został uchylony. W związku z powyższym, kontrolowana jednostka była uprawniona do przetwarzania danych osobowych gości ośrodków wypoczynkowych jedynie w zakresie niezbędnym dla realizacji świadczonych usług, w tym wystawienia faktury.

W toku innej kontroli[66], której poddano wojewódzki ośrodek egzaminowania kierowców stwierdzono, że ww. podmiot przetwarza dane osobowe w zakresie utrwalonych wizerunków oraz głosów kandydatów na kierowców, egzaminatorów, instruktorów oraz osób trzecich, zarejestrowanych za pomocą urządzenia technicznego służącego do zapisu obrazu i dźwięku. Okres przechowywania wskazanych informacji wynosił więcej niż 21 dni od dnia przeprowadzenia egzaminu, wbrew przepisowi art. 54 ust. 2 ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. Nr 30 poz. 151 z późn. zm.)[67]. Ww. termin został przez ustawodawcę określony jako termin maksymalny, po upływie którego (za wyjątkiem wskazanym w art. 54 ust. 4 tej ustawy)[68] ww. dane osobowe winny zostać usunięte. W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu postępowania administracyjnego wydał decyzję, w uzasadnieniu której

[65] Kontrola DIS-K-421/152/13
[66] Kontrola DIS-K-421/40/13
[67] Art. 54 ust. 2. Zapis z praktycznej części egzaminu przechowuje się przez okres 21 dni od dnia przeprowadzenia egzaminu.
[68] Art. 54 ust. 4. W przypadku gdy osoba składająca egzamin złożyła skargę na jego przebieg lub warunki, w jakich był przeprowadzony, zapis jest przechowywany do czasu zakończenia postępowania wyjaśniającego.

wskazał, iż przetwarzanie przez wojewódzki ośrodek szkolenia kierowców danych osobowych w ww. zakresie przez okres dłuższy niż 21 dni od dnia przeprowadzenia egzaminu państwowego było niezgodne z prawem, gdyż narusza art. 54 ust. 2 ustawy o kierujących pojazdami, a obowiązek ich przetwarzania przez dłuższy okres (za wyjątkiem określonym w art. 54 ust. 4 powołanej ustawy) nie znajduje uzasadnienia, gdyż nie wynika z odrębnych przepisów prawa.

2.3. Systemy informatyczne służące do przetwarzania danych osobowych

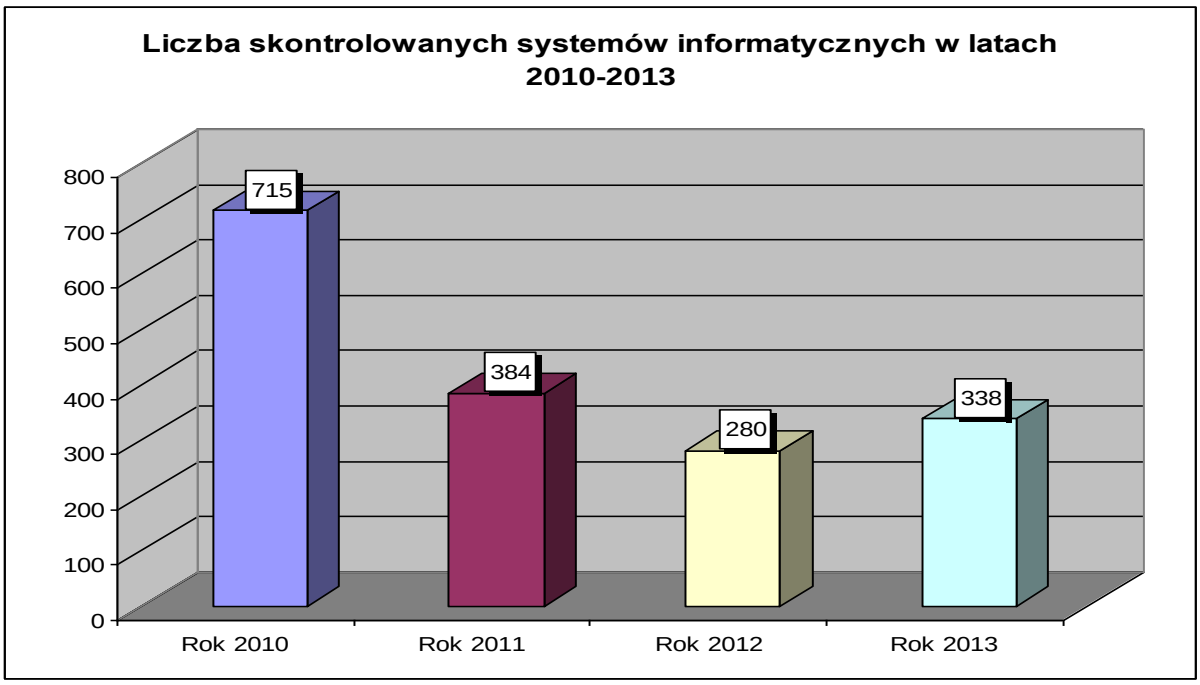
W ramach 165 przeprowadzonych w 2013 r. kontroli, weryfikacji poddano 338 systemy informatyczne wykorzystywane do przetwarzania danych osobowych.

rok 2010 = 187 kontroli, obejmujących 715 systemów informatycznych,

rok 2011 = 188 kontroli, obejmujących 384 systemy informatyczne.

rok 2012 = 162 kontroli, obejmujących 280 systemy informatyczne.

rok 2013 = 165 kontroli, obejmujących 338 systemy informatyczne.



Wykres 1: ***Zestawienie porównawcze liczby skontrolowanych systemów informatycznych w latach 2010-2013.***

Z przedstawionego wykresu wynika, że liczba systemów informatycznych objętych kontrolą w roku 2013 była niższa niż w latach 2010-2011. Spowodowane było m.in. to tym,

że przeprowadzane w 2013 r. kontrole sektorowe dotyczyły sklepów internetowych oraz gospodarki odpadami komunalnymi, gdzie do przetwarzania danych osobowych używane były co do zasady scentralizowane systemy informatyczne. Na mniejszą liczbę skontrolowanych systemów informatycznych miał również wpływ charakter dużej grupy przeprowadzonych kontroli częściowych polegających na sprawdzeniu, czy w przetwarzanych przez kontrolowany podmiot zbiorach danych znajdują się informacje o określonej osobie. W większości przypadków dane te były przetwarzane w specjalistycznych systemach informatycznych dostosowanych funkcjonalnie do ich przetwarzania. Zauważyć należy również, że w wielu podmiotach do przetwarzania danych osobowych używano systemów informatycznych, które często służą do przetwarzania kilku różnych zbiorów danych osobowych. Wskazane wyżej czynniki miały istotny wpływ na mniejszą liczbę sprawdzanych systemów informatycznych.

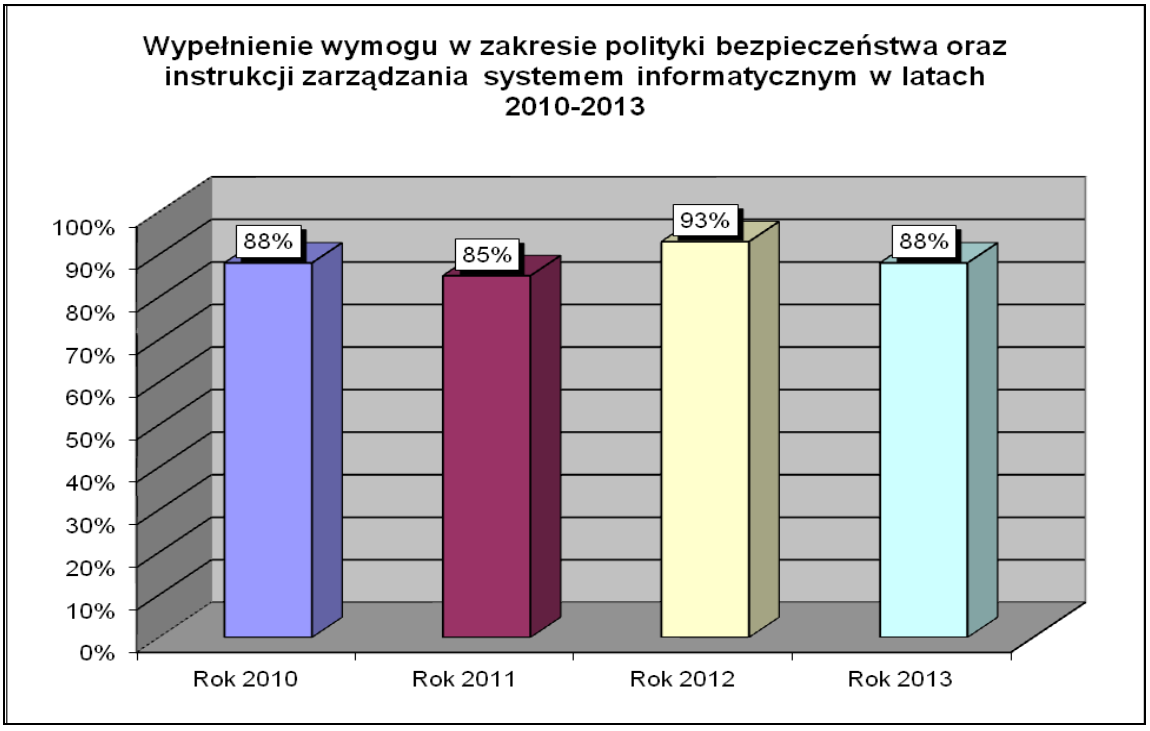
2.4. Wyniki kontroli w zakresie obowiązków formalnych i organizacyjnych

Spełnienie przez kontrolowane podmioty w latach 2010-2013 wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie i rozporządzeniu, zobrazowane zostało 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 odnoszą się do prowadzonej dokumentacji procesu przetwarzania danych, obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, czy też powołania administratora bezpieczeństwa informacji 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.

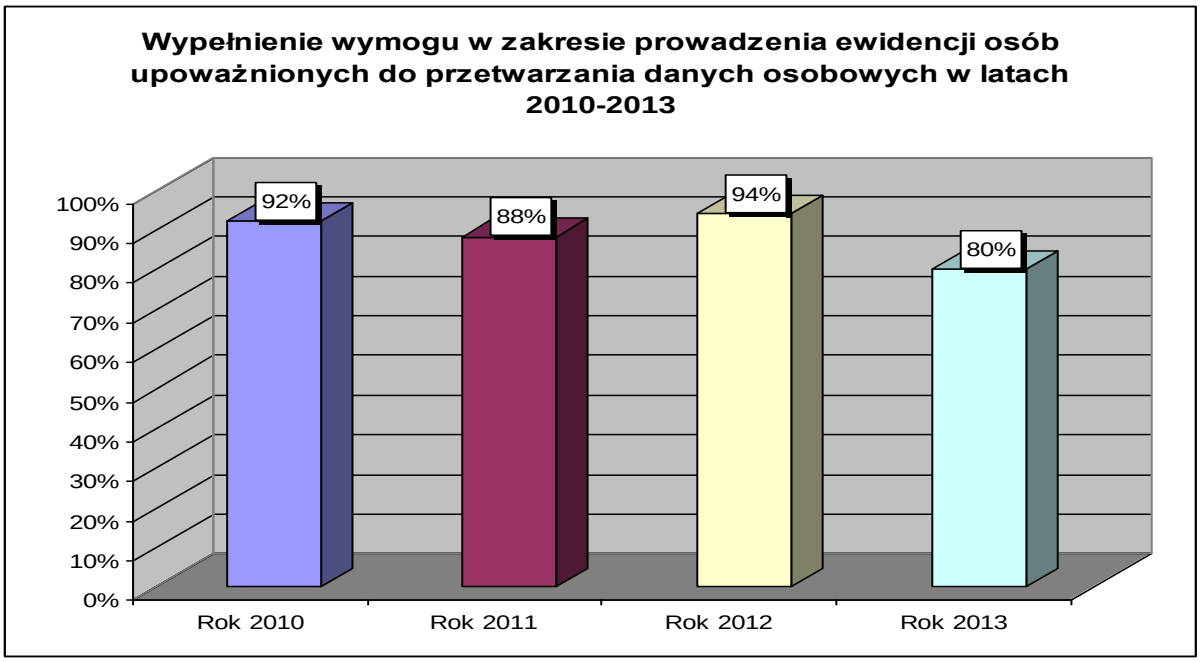
W przypadku, gdy kontrolowana jednostka opracowała wymagane dokumenty (takie jak polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych), prowadziła ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wdrożyła opisane w tej dokumentacji procedury przetwarzanie 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 2010-2013 przedstawiono na poniższych wykresach.

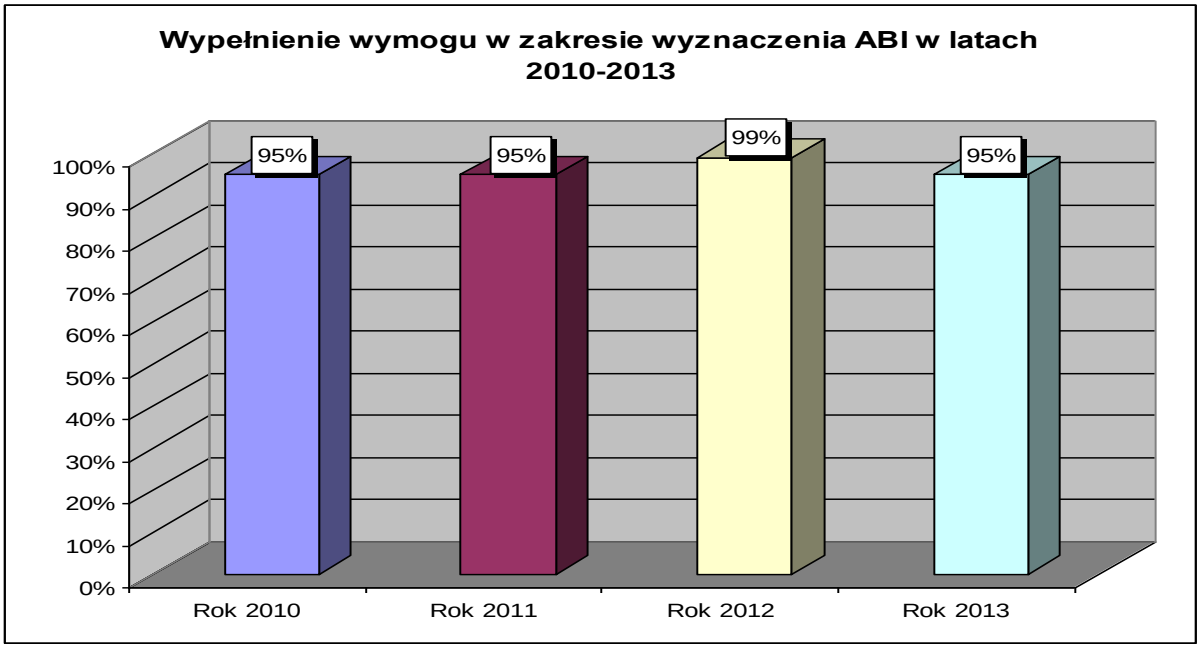


Wykres 2: ***Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych (polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym).***



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

Zbiorcze zestawienie wypełnienia wymogów formalnych i organizacyjnych w latach 2010-2013 w zakresie realizacji obowiązku wyznaczenia osoby pełniącej zadania Administratora Bezpieczeństwa Informacji (ABI), przedstawiono na poniższym wykresie.

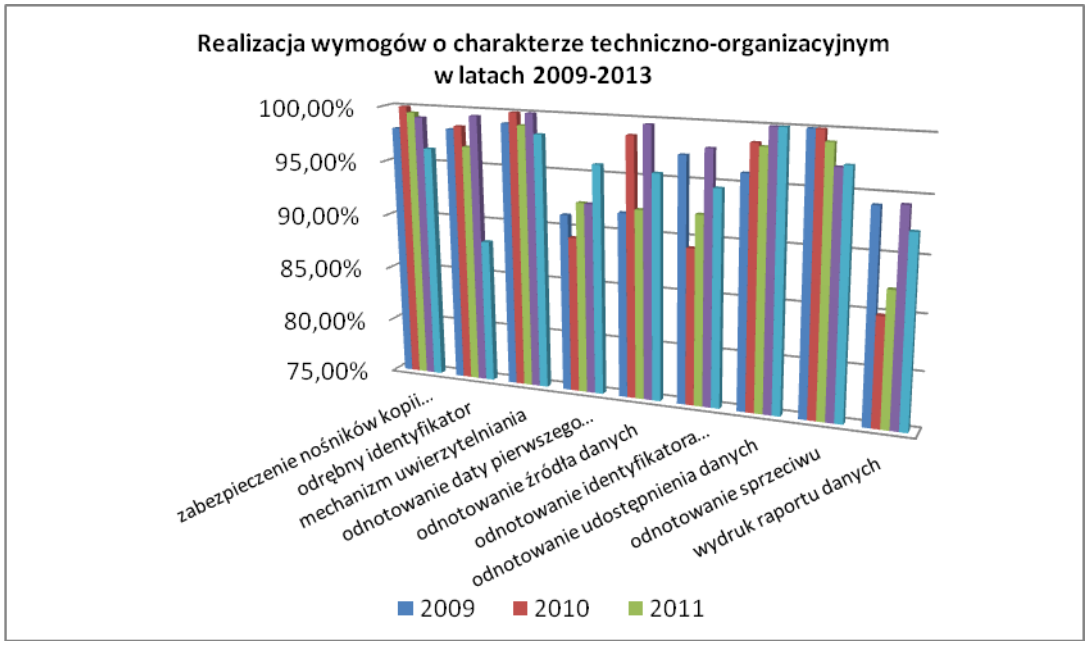


Wykres 4: ***Stopień realizacji obowiązku w zakresie wyznaczenia Administratora Bezpieczeństwa Informacji.***

2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych

Jak już wspomniano, podczas wykonywania czynności kontrolnych w 2013 r. skontrolowano 338 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 jako spełnione. Stopień realizacji wymogów o charakterze techniczno-organizacyjnym dla systemów informatycznych objętych kontrolą w roku 2013 w porównaniu do lat 2010-2012 przedstawiono poniższym wykresie.

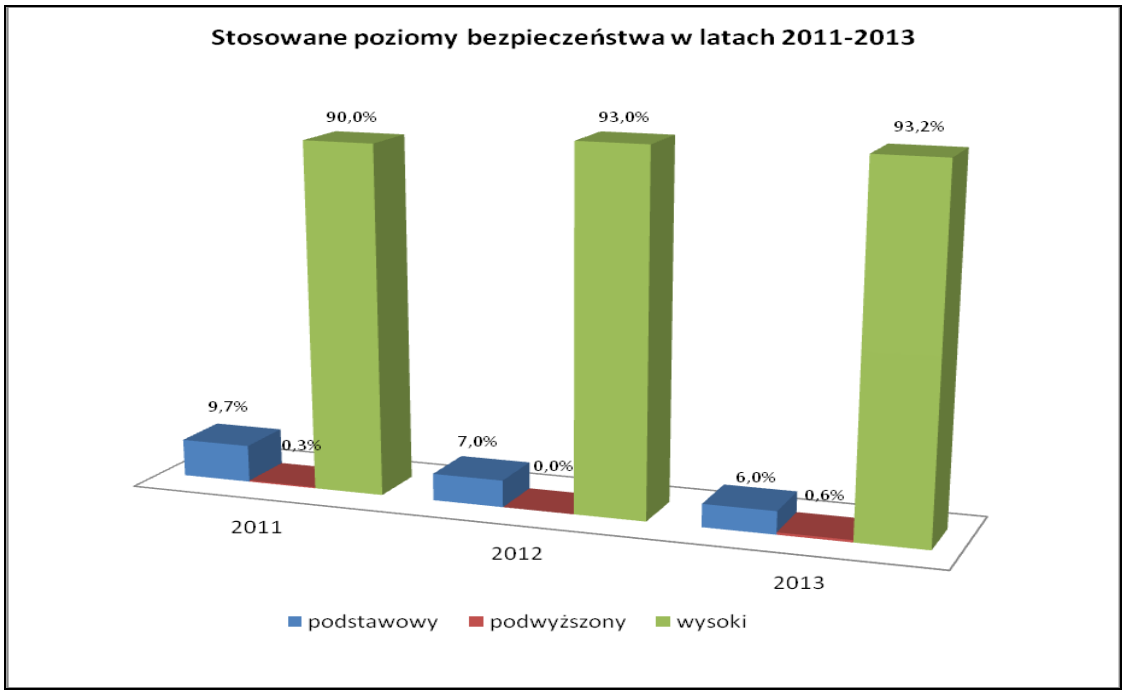


Wykres 5: ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2009-2013.***

Przeprowadzone w 2013 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.

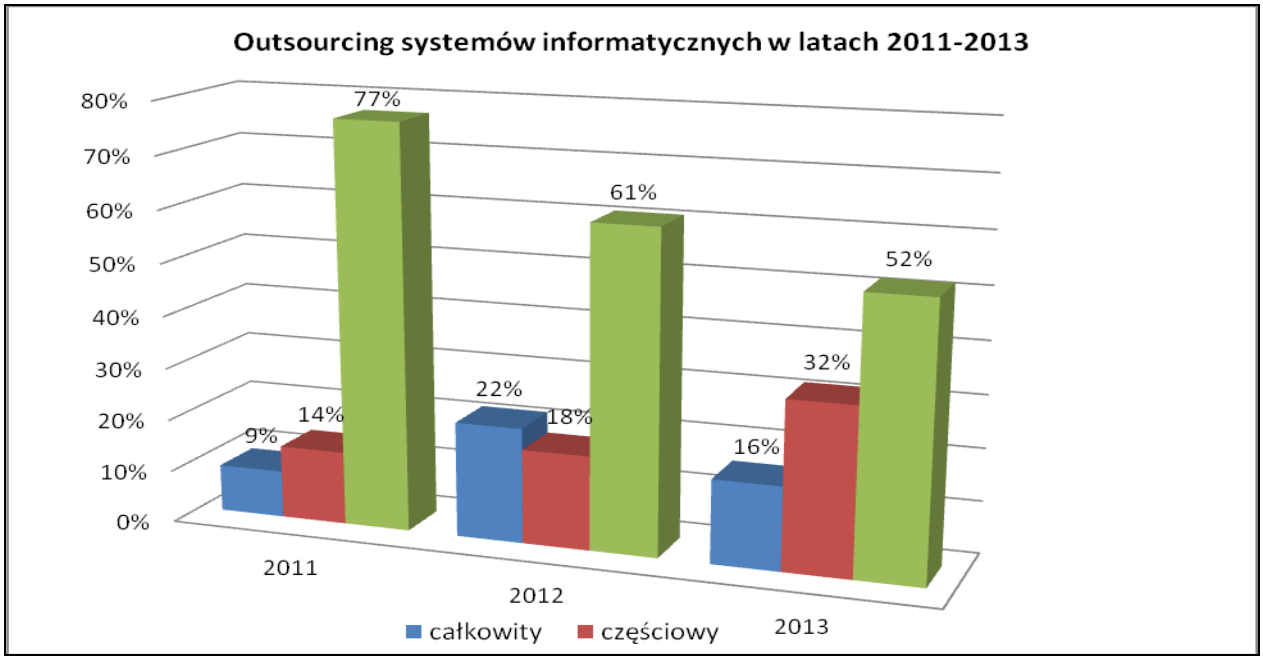
Podział na poziomy bezpieczeństwa w odniesieniu do skontrolowanych w latach 2011-2013 r. systemów informatycznych przedstawiony został na poniższym wykresie.



Wykres 6: ***Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w latach 2011-2013.***

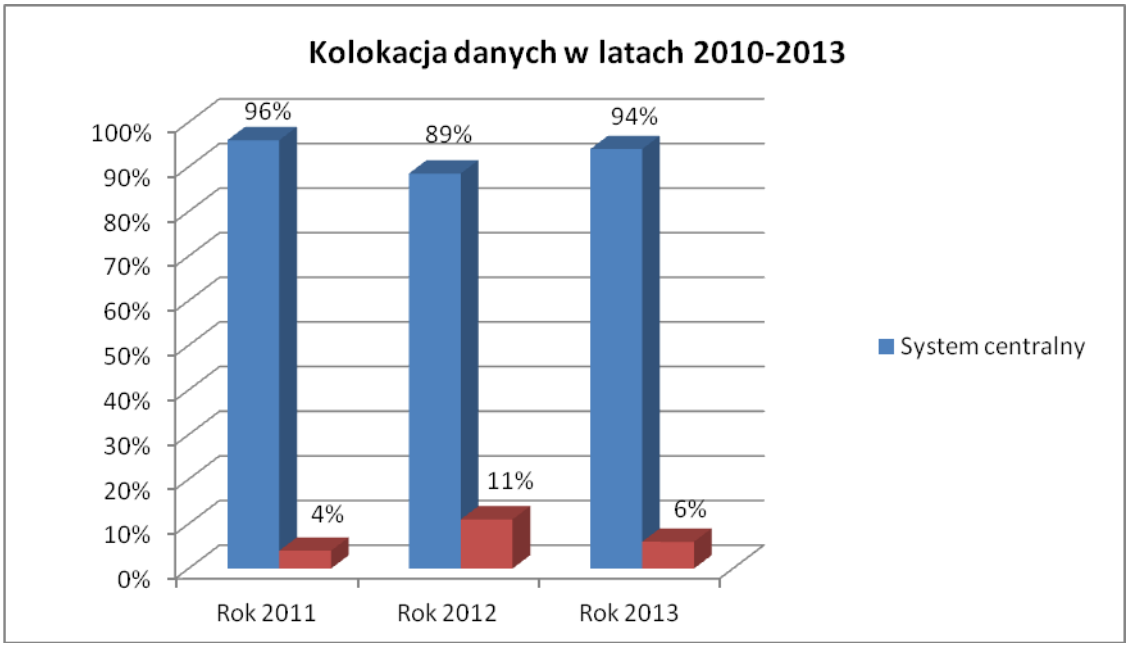
Jak wynika z ww. wykresu, znaczna część podmiotów skontrolowanych w 2013 r. (93,22%) zastosowała wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Stwierdzono również niewielki spadek konieczności stosowania zabezpieczeń na poziomie podstawowym. Wiąże się to z tym, że znakomita większość kontrolowanych systemów informatycznych były to systemy podłączone do sieci Internet, a co za tym idzie - wymaganym zabezpieczeniem dla przetwarzanych za pomocą tych systemów danych jest poziom wysoki. Porównanie wyników kontroli z ostatnich lat wskazuje, że podział zabezpieczeń na poziomy w rozporządzeniu wykonawczym do ustawy, nie oddaje stanu rozwoju systemów w drugim dziesięcioleciu XXI w. Zdecydowana większość kontrolowanych systemów mieści się w jednym z wyznaczanych przez rozporządzenie zakresów.

Jak wynika z przeprowadzonych kontroli większość podmiotów do przetwarzania danych wykorzystuje systemy, nad którymi posiadają 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 2013 r. stosowany był w odniesieniu do około 16 % systemów informatycznych. Zauważono również, że wśród skontrolowanych systemów informatycznych nastąpiło zmniejszenie liczby tych systemów, których obsługą techniczną i administracją zajmowali się pracownicy administratora danych (52% systemów informatycznych). W porównaniu do roku 2012 można zaobserwować znaczącą zmianę 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 odniesieniu do 32% skontrolowanych w 2013 systemów.



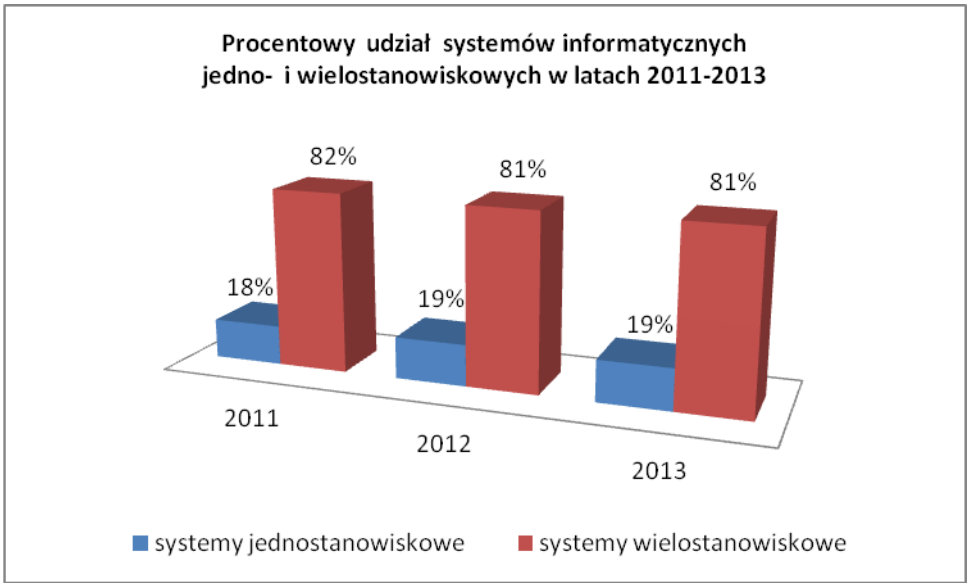
Wykres 7: ***Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2011-2013.***

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 serwerze/serwerach znajdujących się w jednym budynku, zazwyczaj w siedzibie kontrolowanego podmiotu. Zauważyć jednak należy, że w 2013 r. – w stosunku do 2012 roku - zwiększyła się liczba podmiotów wykorzystujących do przetwarzania danych osobowych systemy rozproszone. Na poniższym wykresie przedstawiono zilustrowano stopień zastosowania przez kontrolowane podmioty rozwiązań technicznych opartych o systemy centralne i rozproszone.



Wykres 8: ***Ilościowy udział centralnego/rozproszonego przetwarzania danych w systemach informatycznych objętych kontrolą w latach 2011 - 2013.***

W porównaniu z poprzednimi latami sprawozdawczymi, liczba wykorzystywanych w 2013 r. wielostanowiskowych systemów informatycznych znajdowała się ma zbliżonym poziomie (81%). Rozwiązania oparte o systemy jednostanowiskowe stanowiły niecałe 19% skontrolowanych systemów informatycznych. Zastosowanie systemów jednostanowiskowych w większości przypadków dotyczyło przestarzałych rozwiązań informatycznych. Zauważyć jednak należy, że sięgano po systemy jednostanowiskowe najczęściej w przypadkach, gdy wymagała tego specyfika ich zastosowania (np. systemy monitoringu).



Wykres 9: ***Procentowy udział systemów informatycznych jedno- i wielostanowiskowych wśród systemów objętych kontrolą w latach 2011-2013.***

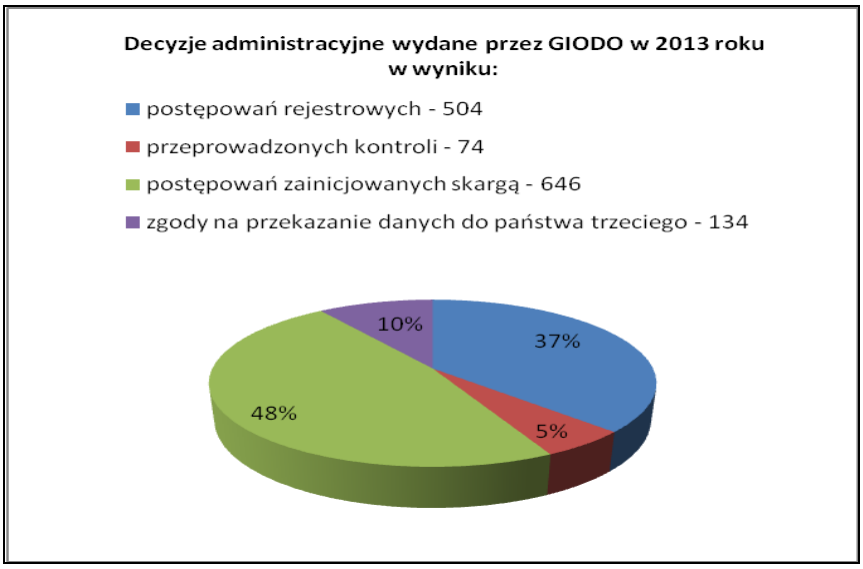
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych

3.1. Wydawanie decyzji

Postępowanie dotyczące naruszenia ustawy o ochronie danych osobowych, wszczęte przez Generalnego Inspektora z urzędu lub na wniosek osoby zainteresowanej, 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 2013 r. Generalny Inspektor wydał **1358 decyzji administracyjnych,** tj. o 61 więcej w stosunku do roku 2012, w którym wydanych było 1297 decyzji. Spośród 1358 decyzji wydanych w 2013 r. **504 dotyczyło postępowań rejestrowych**, **74 zostało wydanych w**

związku z przeprowadzonymi kontrolami, 646 wydano na skutek postępowania zainicjowanego skargą, zaś 134 dotyczyło zgody na przekazanie danych do państwa trzeciego. Pośród 1358 decyzji **109** z nich dotyczyło **egzekucji administracyjnej**.



Wykres 10: ***Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2013 r.***

W obszarze postępowań rejestrowych i przeprowadzonych kontroli odnotować należy nieznaczny wzrost wydanych przez GIODO decyzji. W odniesieniu do postępowań rejestrowych w 2013 r. wydano 504 decyzje, podczas gdy w 2012 – 427, natomiast w sprawach związanych z przeprowadzonymi kontrolami wydano 74 decyzje w 2013 r. i 57 w 2012 r.

Charakterystyczny jest natomiast znaczny, bo ponad dwukrotny wzrost liczby decyzji GIODO w sprawie wniosków o wyrażenie zgody na przekazanie danych osobowych do państwa trzeciego (51 decyzji w 2012 r. i 134 decyzje w 2013 r.) oraz spadek liczby decyzji w odniesieniu do postępowań zainicjowanych skargą (2013 r. – 646 decyzji, 2012 r. – 762 decyzje).

3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych skierował do organów powołanych do ścigania przestępstw **16 zawiadomień**

o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych. W porównaniu z rokiem 2012, w którym wystosowano 12 zawiadomień, stanowi to nieznaczny wzrost.

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 16 zawiadomień skierowanych do organów ścigania, w jednym przypadku dotyczyło ono stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w art. 49 ust. 1 ustawy, przetwarzania danych osobowych w celach marketingowych przez podmioty nieuprawnione. W toku postępowania Generalny Inspektor ustalił, iż spółka nie zaprzestała przetwarzania danych osobowych skarżącego w celach marketingowych, mimo iż przynajmniej dwukrotnie zgłaszał on swój sprzeciw wobec przetwarzania danych w tych celach[69].

Ponadto w 6 przypadkach zawiadomienie dotyczyło przestępstwa wskazanego w art. 51 ustawy, tj. udostępnienia danych osobowych podmiotom nieupoważnionym. W jednej ze spraw wspólnicy spółki cywilnej złożyli skargę na działalność podmiotu, który w przesłanym do współpracujących ze spółką cywilną podmiotów udostępnił dane osobowe jej wspólników w zawiadomieniu zawierającym negatywną ocenę kondycji finansowej spółki cywilnej[70]. Jedno z zawiadomień dotyczyło skargi na udostępnienie przez szpital informacji dotyczących stanu zdrowia skarżącej na rzecz jej pracodawcy[71], zaś kolejne - umożliwienia dostępu do danych osobowych zawartych w dokumentacji pracowniczej przez byłego syndyka masy upadłościowej[72]. W pozostałych 2 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[73].

W dwóch zawiadomieniach GIODO stwierdził wypełnienie znamion czynu zabronionego wskazanego w art. 52 ustawy o ochronie danych osobowych. W jednym z nich Generalny Inspektor podniósł, iż szpital poprzez niedołożenie należytej staranności w zabezpieczeniu dostępu do danych utracił akta osobowe osoby skarżącej zawierające jej

[69] DOLiS/ZAW-3/13/33363
[70] DOLiS/ZAW-1/13/19072
[71] DOLiS/ZAW-6/13/38484
[72] DOLiS/ZAW-7/13/38840
[73] DOLiS/ZAW-2/13/31655, DOLiS/ZAW-15/13/81301.

dane osobowe[74]. Kolejne zawiadomienie dotyczyło naruszenia obowiązku zabezpieczenia danych osobowych przed ich zabraniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem. Kilkudziesięciu pracowników złożyło skargę na przetwarzanie ich danych osobowych zawartych w dokumentacji i systemach informatycznych spółki, polegające na bezprawnym przejęciu tej dokumentacji, w tym akt osobowych, i udostępnieniu ich podmiotom nieupoważnionym[75].

Z kolei 4 zawiadomienia dotyczyły przestępstw wskazanych w art. 51 i art. 52 ustawy o ochronie danych osobowych. W jednym z nich Generalny Inspektor uzyskał informację o porzuceniu w siedzibie spółki koperty z „ważną zawartością" przez jednego z pracowników tego podmiotu[76]. Kolejne dotyczyło wysyłania na adres mailowy skarżącego elektronicznego zestawienia operacji bankowych osób trzecich[77], w innym podniesiono brak zabezpieczenia danych osobowych byłych pracowników spółki zawartych w aktach pracowniczych, które zostały złożone w garażu siedziby jednego z urzędów[78]. Ostatni zaś przypadek dotyczył fizjoterapeuty, który wyrzucił do kosza w wynajmowanym przez siebie mieszkaniu niezabezpieczoną dokumentację medyczną pacjentów, zawierającą m.in. dane o ich stanie zdrowia[79].

W jednym tylko przypadku zawiadomienie dotyczyło przestępstw wskazanych zarówno w art. 51, art. 52 i art. 53 ustawy o ochronie danych osobowych. Niniejsze zawiadomienie dotyczyło udostępnienia przez hotel na rzecz osób nieupoważnionych zapisów monitoringu wizyjnego zawierającego wizerunek skarżącej i wykorzystania go następnie przeciwko niej w postępowaniu sądowym[80].

W innym przypadku, w skutek skargi wniesionej do Generalnego Inspektora Ochrony Danych Osobowych, wystosowane zostało zawiadomienie o podejrzeniu popełnienia przestępstwa określonego w art. 54 ustawy o ochronie danych osobowych. Przestępstwo to polegało na niedopełnieniu przez osoby odpowiedzialne w spółce za przetwarzanie danych osobowych, obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub

[74] DOLiS/ZAW-11/13/56306
[75] DOLiS/ZAW-16/13/83843
[76] DOLiS/ZAW-4/1335799
[77] DOLiS/ZAW-9/13/42354
[78] DOLiS/ZAW-12/13/58981
[79] DOLiS/ZAW-13/13/58971
[80] DOLiS/ZAW-8/13/39130

przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ww. ustawie[81].

Spośród wspomnianych 16 zawiadomień skierowanych w 2013 r. przez GIODO do organów ścigania, tylko jedno miało związek z przeprowadzonymi kontrolami.

Zawiadomienie to było związane z nieudaną próbą przeprowadzania kontroli w jednej ze spółek. W celu zorganizowania przedmiotowej kontroli podjęto telefoniczną próbę kontaktu ze spółką. Z uwagi na to, iż pod numerami telefonów, które zostały pozyskane z Internetu oraz z dokumentacji przekazanej przez prokuraturę rejonową, nikt się nie zgłaszał, informacja o planowanych czynnościach kontrolnych została nagrana na automatyczny aparat zgłoszeniowy. Jednocześnie informacja o planowanych czynnościach kontrolnych została wysłana listem zwykłym za zwrotnym potwierdzeniem odbioru na adres siedziby spółki. Ponadto na podstawie informacji pozyskanych z internetu ustalono, iż spółka może prowadzić swoją działalność gospodarczą również pod dwoma innymi adresami. Podjęte przez Generalnego Inspektora działania w ww. zakresie polegające na próbie przeprowadzenia kontroli nie przyniosły jednak rezultatu. Ustalono jedynie, iż pod adresem wskazanym jako siedziba spółki działalność prowadzi podmiot, który świadczy usługi z zakresu najmu lokalu i odbioru korespondencji, tzw. „biuro wirtualne". Ponadto podmiot ten świadczy usługi udostępniania przedsiębiorcom swojego adresu, jako adresu siedziby m.in. do rejestracji działalności gospodarczej. Na podstawie rozmowy przeprowadzonej z pracownikiem „biura wirtualnego" ustalono, iż spółka korzystała z jego usług. W zawartej pomiędzy podmiotem prowadzącym „biuro wirtualne" a spółką umowie wskazany został adres korespondencyjny spółki. Podjęte działania spowodowały, iż prezes zarządu spółki skontaktował się telefonicznie z Biurem Generalnego Inspektora Ochrony Danych Osobowych i uzgodnił termin kontroli i jej miejsce, tj. Biuro Generalnego Inspektora Ochrony Danych Osobowych. Planowana kontrola nie odbyła się jednak z uwagi na to, iż prezes zarządu spółki nie stawił się w wyznaczonym terminie w Biurze GIODO, ani w kolejnych wyznaczonych mu terminach. Generalny Inspektor uznał, iż powyższe działania prezesa zarządu spółki stanowią utrudnianie wykonania czynności kontrolnych, co wypełnia znamiona czynu zabronionego, o którym mowa w art. 54a ustawy o ochronie danych osobowych[82]. Na podstawie art. 19

[81] DOLiS/ZAW-14/13/66989

[82] tj. kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

ustawy o ochronie danych osobowych[83], Generalny Inspektor skierował do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa. Prokuratura Rejonowa umorzyła jednak dochodzenie w przedmiotowej sprawie wskazując, iż brak było podstaw do stwierdzenia, iż prezes zarządu spółki swoim zachowaniem wypełnił znamiona czynu zabronionego wskazanego w art. 54a ustawy o ochronie danych osobowych.

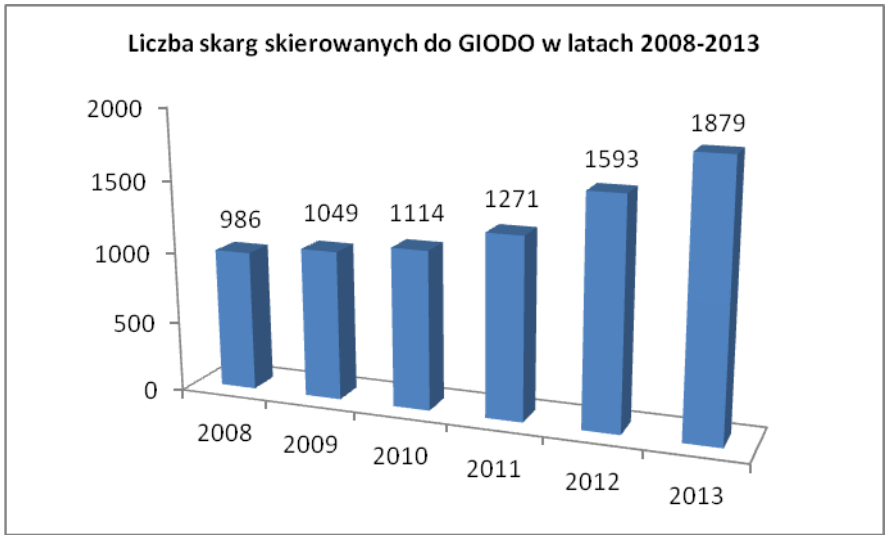
Liczbę zawiadomień o podejrzeniu popełnienia przestępstwa składanych przez Generalnego Inspektora w latach 2008-2013 przedstawia poniższy wykres:

Wykres 11: ***Porównanie liczby zawiadomień o podejrzeniu popełnienia przestępstwa skierowanych przez GIODO do organów ścigania w latach 2008–2013.***

3.3. Rozpatrywanie skarg

W 2013 r. do Biura GIODO wpłynęło **1879 skarg** dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2013, w którym wpłynęły 1593 skargi, liczba ta uległa **zwiększeniu o 286,** co przedstawia poniższy wykres.

[83] tj. 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



Wykres 12: ***Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008–2013.***

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. W związku z nieuzupełnieniem braków formalnych, w 2013 r. **129 skarg zostało zwróconych** do wnioskodawców. Wiele skarg zostało również pozostawionych bez rozpoznania.

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 omawianym roku sprawozdawczym

GIODO w drodze decyzji administracyjnej **odmówił** uwzględnienia wniosku w **321** sprawach, **75** razy **nakazywał** przywrócenie stanu zgodnego z prawem, zaś w **114** przypadkach **umorzył** postępowanie administracyjne zainicjowane skargą.

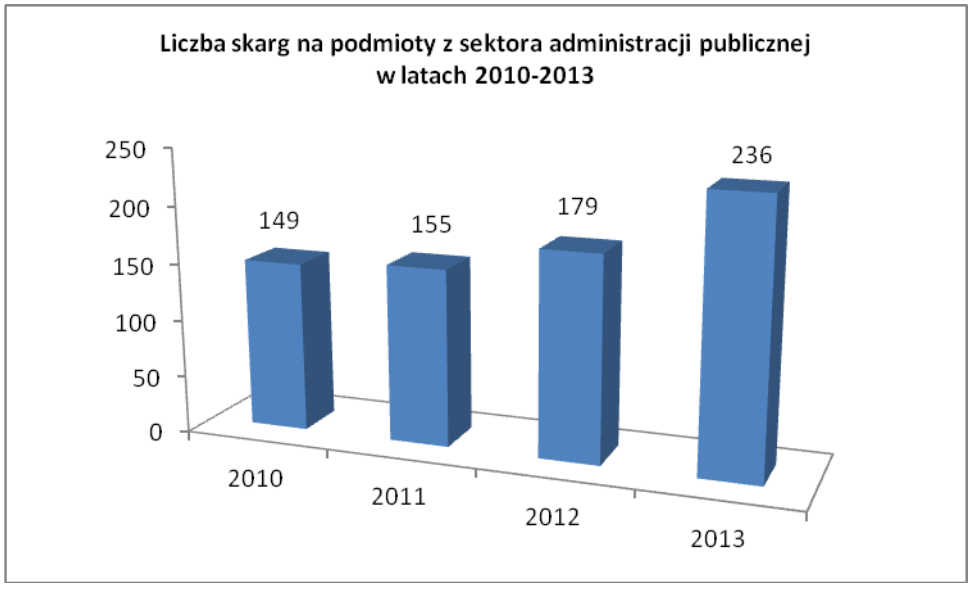
Analizując treść skarg wyróżnić należy 11 podstawowych kategorii, w zależności od zagadnień, których dotyczyły: 1) administracja publiczna, 2) bezpieczeństwo publiczne, 3) sądy, prokuratura, komornicy, 4) organizacje społeczne, 5) banki i inne instytucje finansowe, 6) Internet, 7) marketing, 8) mieszkalnictwo, 9) oświata i szkolnictwo wyższe, 10) służba zdrowia, 11) ubezpieczenia społeczne, majątkowe i osobowe, 12) telekomunikacja, 13) zatrudnienie, 14) windykacja, 15) inne.

Wykres 13: ***Zestawienie porównawcze liczby skarg, które wpłynęły do Biura GIODO w 2013 r. w określonych sektorach.***

Poniżej przedstawione zostały przykłady skarg, które wpłynęły w 2013 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych na podmioty działające w wybranych obszarach.

1) Administracja publiczna

W roku 2013 wpłynęło **236** skarg dotyczących sektora **administracji publicznej**, tj. o 57 więcej niż w roku 2012, w którym wpłynęło 179 skarg z tego zakresu.



Wykres 14: ***Zestawienie porównawcze liczby skarg na podmioty z sektora administracji publicznej, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2013.***

W omawianym okresie GIODO wydał decyzję umarzającą postępowanie w części dotyczącej: a) nieudzielenia skarżącemu przez dyrektora urzędu kontroli skarbowej w B. informacji o tym, kto i na podstawie jakich przepisów sporządził imienne upoważnienie, na podstawie którego spółka z o.o. udostępniła jego dane osobowe, b) dopuszczalności przetwarzania danych osobowych przez dyrektora urzędu kontroli skarbowej w P. i Ministra Finansów, c) dopuszczalności przetwarzania przez dyrektora urzędu kontroli skarbowej w B. danych osobowych skarżącego udostępnionych przez spółkę akcyjną; nakazującą: a) dyrektorowi urzędu kontroli skarbowej w B. spełnienie wobec skarżącego obowiązku informacyjnego, o którym mowa w art. 33 ustawy o ochronie danych osobowych, poprzez poinformowanie go na piśmie, jakie jego dane osobowe zawiera zbiór, w jaki sposób je zebrano i od kiedy są przetwarzane w zbiorze, cel i zakres przetwarzania tych danych, a także w jakim zakresie oraz komu zostały udostępnione, za wyjątkiem informacji, w stosunku do których obowiązek ich przekazania jest wyłączony przez przepisy ustawy o ochronie danych osobowych, b) spełnienie przez spółkę akcyjną obowiązku informacyjnego wobec skarżącego, o którym mowa w art. 33 ustawy o ochronie danych osobowych, poprzez poinformowanie go na piśmie, w jakim zakresie jego dane osobowe zostały udostępnione

dyrektorowi urzędu kontroli skarbowej w B.; zaś w pozostałym zakresie odmawiającą uwzględnienia wniosku[84].

Z treści skargi wynikało, iż skarżący, stosownie do art. 33 ustawy o ochronie danych osobowych, zwrócił się do urzędu kontroli skarbowej w B. o udzielenie mu w formie pisemnej informacji o posiadanych przez ten podmiot jego danych osobowych, ale w odpowiedzi całkowicie pominięto jego żądanie w tym zakresie. Skarżący wskazał, że jego zdaniem było to spowodowane chęcią ukrycia dowodów potwierdzających fakt zdobycia jego danych osobowych w sposób niezgodny z przepisami prawa przed wszczęciem postępowania kontrolnego, oraz że *„(...) moje dane osobowe mógł pozyskać inspektor urzędu kontroli skarbowej po okazaniu imiennego upoważnienia do prowadzenia postępowania kontrolnego. Datą wszczęcia postępowania jest dzień, w którym doręczono mi postanowienie o wszczęciu postępowania, natomiast moje dane osobowe znajdujące się na portalu A. ustalono przed wszczęciem postępowania"*. Skarżący wskazał również, że urząd kontroli skarbowej w B. w swoim piśmie jednoznacznie powołuje się na artykuł 36 ustawy o kontroli skarbowej, co jego zdaniem oznacza, że jeśli użyto wywiadu skarbowego przed wszczęciem postępowania, to rażąco naruszono przepisy prawa.

Podsumowując skarżący zakwestionował, po pierwsze, legalność pozyskania jego danych osobowych od jednego z banków, ponieważ w jego opinii niezgodnie z przepisami wezwano go do ujawnienia danych bankowych na podstawie art. 155 Ordynacji podatkowej, zaś wezwanie zostało sporządzone przed wszczęciem postępowania przez osobę nieuprawnioną. Skarżący podniósł, że momentem wszczęcia postępowania jest doręczenie stosownego postanowienia i upoważnienia przez inspektora. Wskazał również, że w jego obecności po wszczęciu postępowania wezwanie to nie zostało sporządzone i podpisane, tylko doręczone z odręcznie dopisaną datą oraz że zgodnie z art. 33a ustawy o kontroli skarbowej upoważnionym do wezwania jest dyrektor urzędu kontroli skarbowej po zapoznaniu się z zebranym materiałem dowodowym. Ponadto do dnia dzisiejszego nie otrzymał od urzędu kontroli skarbowej w B. odpowiedzi na swoje pismo, w którym wniósł o podanie powodów, dla których ma zrezygnować z prawa do ochrony tajemnicy bankowej na korzyść ww. dyrektora tego urzędu.

[84] Decyzja GIODO z 19 lipca 2013 r. DOLiS/DEC-762/13/46046,46056,46063,46077,46085,46093,46102.

Po drugie, skarżący podważał legalność pozyskania przed wszczęciem postępowania przez urząd kontroli skarbowej w B. od spółki z o.o. jego danych osobowych, identyfikujących go jako użytkownika o wskazanym w toku postępowania nicku. Sygnalizował, że obowiązujący wówczas art. 7b ustawy o kontroli skarbowej jednoznacznie wskazywał, iż dane można udostępnić na podstawie imiennego upoważnienia organu kontroli skarbowej oraz zarzucił, iż imienne upoważnienie organu kontroli skarbowej sporządzono w urzędzie kontroli skarbowej w B., natomiast jego dane osobowe zostały przekazane wcześniej, do urzędu kontroli skarbowej w P. Skarżący zarzucił również, że nie wie, gdyż jest to ukrywane przed nim, kto i na podstawie jakich przepisów sporządził imienne upoważnienie organu kontroli skarbowej, na podstawie którego „A.” przekazało jego dane osobowe do urzędu kontroli skarbowej w P.

Skarżący zakwestionował również legalność pozyskania przez urząd kontroli skarbowej w B. z „A.”, przed wszczęciem postępowania, jego danych osobowych zawartych w zestawieniu aukcji odbytych na „A.”, które zostało włączone do akt postępowania kontrolnego postanowieniem. Skarżący zarzucił, że stwierdzenie, iż dane te pochodzą z określonej strony internetowej jest nieprawdziwe. A ponieważ wykazał, iż na stronie tej nie ma tych danych, wskazano na inny serwis, więc skarżący znów udowadniał, że strona pod tym adresem nie była dostępna w trakcie prowadzonego postępowania. Zarzucił ponadto, że do dnia dzisiejszego urząd kontroli skarbowej w B. ukrywa fakt pozyskania przed wszczęciem postępowania danych niedostępnych publicznie, a znajdujących się w posiadaniu „A.”;

Skarżący zanegował również legalność pozyskania jego danych osobowych ze spółki akcyjnej. Urząd kontroli skarbowej w B. odmawiał włączenia tych danych do akt postępowania, natomiast spółka ta bezzasadnie zasłaniała się Prawem pocztowym. Wskazał również, że ze względu na przepisy Prawa pocztowego spółka akcyjna powinna odmówić jakichkolwiek działań na rzecz urzędu kontroli skarbowej w B., natomiast on - na mocy art. 33 ustawy o ochronie danych osobowych - ma prawo do zapoznania się z tym, jakie dane dotyczące jego osoby zostały udostępnione urzędowi w B., o co dwukrotnie zwracał się do tego podmiotu.

W trakcie postępowania Generalny Inspektor ustalił, iż w zakresie zarzutu skarżącego dotyczącego nieudzielenia przez dyrektora urzędu kontroli skarbowej w B. informacji o tym, kto i na jakiej podstawie jakich przepisów sporządził imienne upoważnienie na podstawie

którego spółka z o.o. udostępniła jego dane osobowe – wskazany organ nie przetwarzał tych informacji. W związku z powyższym w tej części postępowanie stało się bezprzedmiotowe i należało je umorzyć. Również wyjaśnienia dyrektora urzędu kontroli skarbowej w P. i Ministerstwa Finansów, potwierdziły, iż oba podmioty nie przetwarzały danych osobowych skarżącego udostępnionych przez spółkę z o.o. i postępowanie również w tym zakresie stało się bezprzedmiotowe. Z uwagi na fakt, iż aktualnie dyrektor urzędu kontroli skarbowej w B. nie przetwarza danych osobowych skarżącego udostępnionych mu przez spółkę akcyjną, postępowanie również w zakresie dopuszczalności przetwarzania tych danych stało się bezprzedmiotowe.

Z zebranego w sprawie materiału dowodowego wynikało, że skarżący zwrócił się o udzielenie w formie pisemnej informacji wskazanych w art. 33 ust. 1 pkt 1-4 ustawy, natomiast w ocenie Generalnego Inspektora nie daje to podstaw do przyjęcia, że zaistniały przesłanki uzasadniające kompleksowe nieudzielenie przez dyrektora urzędu kontroli skarbowej w B. żądanych przez skarżącego informacji. GIODO uznał, że niezasadne było potraktowanie wskazanego w udzielonej skarżącemu przez dyrektora ww. urzędu w B. odpowiedzi, art. 7b ustawy z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2004 r. Nr 8, poz. 65 z późn. zm.), jako przepisu uchylającego w całości obowiązek wynikający z art. 33 ust. 1 ustawy o ochronie danych osobowych. Dyrektor urzędu kontroli skarbowej w B. w chwili, gdy skarżący zwrócił się o udzielenie informacji dotyczących przetwarzania jego danych osobowych, przetwarzał dotyczące go informacje nie objęte dyspozycją art. 7b zdanie trzecie ustawy o kontroli skarbowej, np. informacje pochodzące z ogólnodostępnych stron internetowych. Okoliczności niniejszej sprawy nie wskazywały również, aby dotyczące skarżącego informacje pochodzące od spółki z o.o. były objęte dyspozycją art. 7b zdanie trzecie ustawy o kontroli skarbowej. To, że inspektor kontroli skarbowej wykonujący swoje obowiązki w urzędzie kontroli skarbowej w P. przekazał zapytanie do wspomnianej spółki z o.o. drogą elektroniczną, jak również fakt, iż dyrektor urzędu kontroli skarbowej w P. nie udzielił imiennego upoważnienia w sprawach dotyczących zapytań otrzymywanych z Ministerstwa Finansów na podstawie art. 7b ustawy o kontroli skarbowej, wskazuje bowiem że nie zaistniał tryb określony w art. 7b zdanie drugie ustawy o kontroli skarbowej.

W ocenie Generalnego Inspektora poinformowanie skarżącego, jakie jego dane osobowe znajdują się zbiorze danych, którego administratorem jest dyrektor urzędu kontroli skarbowej w B., w jaki sposób zebrano te dane, w jakim celu i zakresie są one przetwarzane,

w jakim zakresie oraz komu zostały udostępnione, nie spowodowałoby również wystąpienia okoliczności wymienionych w art. 30 pkt 2 i 3 ustawy, takich jak zaistnienie zagrożenia dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, czy też zagrożenia dla podstawowego interesu gospodarczego lub finansowego państwa. Dyrektor urzędu kontroli skarbowej w B. niezasadnie nie przekazał skarżącemu informacji, o udzielenie których występował on w swoim piśmie. W ocenie Generalnego Inspektora po stronie ww. podmiotu zaistniały uchybienia przy wypełnianiu wobec skarżącego obowiązku informacyjnego określonego w art. 33 ustawy.

Wobec powyższego zasadne było - stosownie do dyspozycji art. 18 ust. 1 pkt 1 ustawy - nakazanie dyrektorowi urzędu kontroli skarbowej w B. usunięcia tych uchybień. Jednocześnie podkreślić należy, że nakaz ten nie odnosił się do informacji, w stosunku do których obowiązek ich przekazania był wyłączony przez przepisy ustawy o ochronie danych osobowych. Odnośnie odmowy udzielenia przez spółkę akcyjną wnioskowanych przez skarżącego informacji, Generalny Inspektor stanął na stanowisku, iż mające zastosowanie do oceny tej kwestii art. 33 i art. 32 ust. 1 pkt 1-5 ustawy, nie nakładały na ww. podmiot obowiązku udzielenia informacji o tym, czy urząd kontroli skarbowej w B. zwracał się z żądaniami o udzielenie jakichkolwiek informacji o skarżącym, jakie są daty i sygnatury pism urzędu kontroli skarbowej w B., na podstawie jakich przepisów prawa formułowano żądania, czy grożono odpowiedzialnością karną lub innymi karami w przypadku niezastosowania się do żądań i jaki był zakres żądanych informacji.

W ocenie Generalnego Inspektora na gruncie przepisów o ochronie danych osobowych skarżący nie mógł się również domagać udostępnienia mu kopii korespondencji prowadzonej pomiędzy urzędem kontroli skarbowej w B. a P. Zdaniem Generalnego Inspektora nie zaistniała żadna z przesłanek wskazanych w wówczas obowiązującym art. 30 ustawy, która wyłączałaby realizację tego obowiązku. Poinformowanie skarżącego o zakresie jego danych osobowych udostępnionych na rzecz dyrektora urzędu kontroli skarbowej w B. nie spowodowałoby ujawnienia wiadomości stanowiących tajemnicę państwową, zagrożenia dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego, zagrożenia dla podstawowego interesu gospodarczego lub finansowego państwa, czy też istotnego naruszenia dóbr osobistych skarżącego lub innych osób. Odmowa udostępnienia skarżącemu tej informacji naruszała przepisy o ochronie danych osobowych, a zatem zasadne było nakazanie spółce akcyjnej usunięcia uchybienia w tym zakresie.

Odnośnie zebrania przez dyrektora urzędu kontroli skarbowej w B. danych osobowych skarżącego od banku, w opinii Generalnego Inspektora takie działanie znajdowało oparcie w przesłance określonej w przytoczonym powyżej art. 23 ust. 1 pkt 2 ustawy. Przepisem, z którego wynikało uprawnienie ww. dyrektora i obowiązek banku, dla zrealizowania których niezbędne było przetwarzanie danych osobowych skarżącego w kwestionowany przez niego sposób, był art. 33a ust. 1 ustawy o kontroli skarbowej. Z kolei w odniesieniu do danych osobowych skarżącego zebranych przez dyrektora urzędu kontroli skarbowej w B., a pochodzących od spółki z o.o., Generalny Inspektor stanął na stanowisku, iż zebranie tych danych również było dopuszczalne, tak samo jak zebranie przez ww. dyrektora dotyczących skarżącego informacji udostępnionych przez bank, które były zawarte w zestawieniach zakończonych aukcji skarżącego odbytych w serwisie A. i informacji udostępnionych przez spółkę z o.o., a także przetwarzanie danych osobowych skarżącego w zbiorze o nazwie „Rejestr podmiotów zobowiązanych do świadczeń na rzecz budżetu państwa". Wobec tego brak było w tym zakresie podstaw do zastosowania środków o których mowa w art. 18 ust. 1 ustawy, co powoduje, że zasadna była odmowa uwzględnienia wniosku.

W 2013 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga dotycząca **udostępnienia danych osobowych skarżących w Biuletynie Informacji Publicznej gminy zawartych w uchwałach rady miasta**[85].

Dane osobowe skarżących znalazły się w dwóch dokumentach opublikowanych w BIP gminy. Skarżący wskazali, iż zwracali się do rady miasta o zastąpienie ich nazwisk inicjałami, lecz spotkali się z dwukrotną odmową. W toku postępowania przeprowadzonego przez Generalnego Inspektora dane osobowe skarżących zostały usunięte (zastąpione inicjałami). Pomimo tego Generalny Inspektor Ochrony Danych Osobowych wystąpił do urzędu miasta w celu zasygnalizowania, iż w przedmiotowej sprawie niewątpliwie doszło do uchybień w procesie przetwarzania danych osobowych skarżących przez urząd gminy, poprzez udostępnienie ich danych osobowych, jako osób składających skargę na działania burmistrza, na stronie internetowej BIP gminy oraz zasygnalizował konieczność przestrzegania przepisów ustawy o ochronie danych osobowych poprzez zaprzestanie stosowania ww. praktyki[86].

[85] DOLiS-440-100/13
[86] Pismo GIODO z dnia 14 sierpnia 2013 r. DOLiS-440-100/13/51814.

2) Bezpieczeństwo publiczne

W analizowanym okresie do GIODO wpłynęły **72** skargi dotyczące sektora **bezpieczeństwa publicznego**.

W dniu 31 października 2013 roku Generalny Inspektor Ochrony Danych Osobowych wydał **decyzję odmawiającą uwzględnienia wniosku w zakresie przetwarzania danych osobowych przez Straż Miejską**, a w pozostałym zakresie umorzył postępowanie[87].

Skarżąca podniosła, iż Straż Miejska prowadziła akcję usuwania samochodów zaparkowanych w pobliżu jednego z targowisk, na skutek czego jej samochód został odholowany na posesję prywatną. W prywatnej firmie skarżąca uiściła wysoką opłatę za odholowanie i przechowywanie samochodu. Następnie przyjęła mandat karny w siedzibie Straży Miejskiej, gdzie funkcjonariusz Straży sporządził protokół zawierający jej dane osobowe pochodzące z trzech dokumentów: z dowodu osobistego, prawa jazdy i dowodu rejestracyjnego samochodu. Pozyskano również dane osobowe w zakresie m.in. nazwiska panieńskiego matki skarżącej. W związku z powyższym, skarżąca zwróciła się do Generalnego Inspektora z prośbą o pomoc i skuteczną interwencję w celu niezwłocznego usunięcia jej danych osobowych przetwarzanych przez ww. prywatną firmę oraz spowodowanie, by podobne praktyki stosowane przez Straż Miejska nie mogły mieć miejsca w przyszłości. Ponadto skarżąca wniosła o zbadanie procesu legalności przetwarzania jej danych osobowych przez Straż Miejską.

Organ ds. ochrony danych osobowych wskazał w przedmiotowej decyzji, że Straż Miejska pozyskała dane osobowe skarżącej w związku z wykonywaniem obowiązków nałożonych ustawą, w wyniku podjętych czynności związanych z nieprawidłowym zaparkowaniem pojazdu przez skarżącą. Uznać zatem należało, że Straż Miejska miała prawo pozyskać i przetwarzać dane osobowe skarżącej, a przesłanką legalizującą ten proces jest art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Ponadto prywatna firma (w okresie, którego dotyczy skarga) była stroną umowy z miastem dotyczącej usuwania pojazdów z dróg publicznych i ich umieszczania na parkingu strzeżonym. Umowa ta została zawarta pomiędzy tą firmą oraz Zarządem Dróg i Komunikacji (aktualnie: Zarząd Dróg i Utrzymania Miasta; dalej Zarząd Dróg), jako jednostką wyznaczoną zarządzeniem Prezydenta miasta do usuwania pojazdów i ich umieszczania na parkingu strzeżonym. Jednocześnie w zakresie udostępnienia danych osobowych skarżącej przez Straż Miejską na rzecz prywatnej firmy wskazać należy, że jedyny dokument, jaki został

[87] Decyzja GIODO z dnia 31 października 2013 r. DOLiS/DEC-1148/13/72280,72282,72289.

udostępniony przez Straż Miejską ww. podmiotowi to dyspozycja usunięcia pojazdu skarżącej, zawierająca dane dotyczące pojazdu. Jednakże w ocenie organu dane takie, jak marka i nr rejestracyjny samochodu stanowią dane osobowe. Pozyskanie zaś przez firmę prywatną pozostałych danych skarżącej nastąpiło poprzez przedstawienie przez nią samą zezwolenia na odbiór pojazdu, które w związku z upływem roku od zdarzenia zostało zniszczone. Straż Miejska działała zgodnie z przepisami ustawy o ochronie danych osobowych i brak było podstaw do zastosowania przepisu art. 18 ust. 1 ww. ustawy o ochronie danych osobowych.

W analizowanym okresie sprawozdawczym organ do spraw ochrony danych osobowych rozstrzygał w sprawie **skargi na niewypełnienie wobec skarżącego przez Komendanta Głównego Policji obowiązku informacyjnego określonego w art. 32 ustawy o ochronie danych osobowych,** odnośnie przetwarzania jego danych w Krajowym Systemie Informacyjnym Policji (KSIP). Skarżący podniósł, że zwrócił się do Komendanta o udzielenie informacji odnośnie przetwarzania jego danych osobowych w KSIP, na które udzielono mu odpowiedzi, która nie zawierała wnioskowanych przez niego informacji.

W związku z powyższym skarżący wystosował wobec organu ochrony danych osobowych wniosek o nakazanie przywrócenia stanu zgodnego z prawem, poprzez zobowiązanie Komendanta Głównego Policji do wykonania obowiązku informacyjnego, nałożonego art. 32 ustawy o ochronie danych osobowych. W tym stanie faktycznym Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną, mocą której nakazał Komendantowi usunięcie uchybień w procesie przetwarzania danych osobowych skarżącego poprzez spełnienie wobec niego obowiązku informacyjnego w zakresie wskazanym w art. 33 ust. 1 ustawy o ochronie danych osobowych[88].

3) Sądy, prokuratura, komornicy

W 2013 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **48** skarg dotyczących sektora **sądów, prokuratur i komorników**.

W jednej ze spraw prowadzonych przez organ do spraw ochrony danych osobowych w 2013 r. skarżąca podniosła **okoliczność udostępnienia przez sąd rejonowy opinii o jej stanie zdrowia na rzecz radcy prawnego, niesprostowanie tej opinii przez sąd rejonowy**

[88] Decyzja GIODO z dnia 24 stycznia 2013 r. (znak: DOLiS/DEC-71/13/4394,4396) utrzymana w mocy decyzją GIODO z dnia 13 czerwca 2013 r. znak: DOLiS/DEC-625/13/37430,37431.

oraz na jej udostępnienie przez Radcę na rzecz innego sądu rejonowego. Skarżąca, uzupełniając skargę, wniosła o wydanie decyzji administracyjnej stwierdzającej, że doszło do naruszenia ustawy o ochronie danych osobowych, nakazanie sądowi rejonowemu zastosowanie dodatkowych zabezpieczeń, nakazanie radcy usunięcia uchybień poprzez wycofanie opinii z akt sprawy prowadzonej przed innym sądem rejonowym, nakazanie sądowi oraz radcy sprostowania nieprawdziwych danych w tej opinii i naprawienia wszystkich szkód wynikłych z naruszenia ustawy o ochronie danych osobowych, w tym krzywdy moralnej lub innych.

W związku z przeprowadzonym postępowaniem Generalny Inspektor Ochrony Danych Osobowych wydał decyzję odmawiającą uwzględnienia wniosku[89]. Podniósł bowiem, że udostępnienie przez sąd rejonowy dotyczących skarżącej informacji zawartych w treści sprawozdania pełnomocnikowi reprezentującemu go w postępowaniu sądowym z powództwa skarżącej i udostępnienie tych informacji przez radcę prawnego, jako pełnomocnika strony, na rzecz sądu przed którym postępowanie się toczyło, niewątpliwie znajduje uzasadnienie w przesłance określonej w art. 27 ust. 2 pkt 5 ustawy o ochronie danych osobowych. Jednocześnie podkreślone zostało, że to, czy przekazanie konkretnych dowodów, było w prowadzonym postępowaniu uzasadnione znajduje się poza zakresem kompetencji Generalnego Inspektora. Postępowanie dowodowe w procesie cywilnym zostało uregulowane przepisami ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2014 r. poz. 101), zwanej dalej K.p.c. Zgodnie z art. 233 § 1 K.p.c. to sąd ocenia wiarygodność i moc dowodów według własnego przekonania, na podstawie wszechstronnego rozważenia zebranego materiału. Od orzeczeń sądu przysługują środki odwoławcze. Generalny Inspektor nie jest zaś 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.

Kolejna skarga dotyczyła **przetwarzania danych osobowych przez Zastępcę Komendanta Placówki Straży Granicznej oraz Oddział Straży Granicznej**. Skarżąca podniosła, że była świadkiem w procesie cywilnym w sądzie okręgowym oraz, że pełnomocnik jednej ze stron posiadał wszystkie jej adresy zameldowania od 1993 r., w tym

[89] Decyzja GIODO z dnia 9 kwietnia 2013 r. DOLiS/DEC-407/13/22129,22133,22138,22143.

adres jej czasowego zameldowania. Skarżąca wskazała, że w związku z tym, że w sprawę zaangażowani byli funkcjonariusze Straży Granicznej i Policji, ma uzasadnione obawy, że doszło do udostępnienia jej danych osobowych we wskazany przez nią w skardze sposób właśnie przez którąś z tych formacji, po ich poprzednim pozyskaniu z bazy PESEL. Precyzując skargę skarżąca wskazała, iż Zastępca Komendanta Placówki Straży Granicznej przekazał dane dotyczące jej miejsca zamieszkania w odpowiedzi na pismo jednego z wydziałów cywilnego rodzinnego sądu okręgowego. Skarżąca podniosła również, że Komendant Oddziału Straży Granicznej udzielił odpowiedzi na ponowny wniosek ww. sądu udostępniając jej dane dotyczące miejsca zamieszkania, czasu urlopów i planowanego miejsca przebywania oraz numer telefonu podanego do kontaktu w trakcie przebywania na urlopie. Skarżąca zarzuciła, że jej pracodawca naruszył tym samym jej dobra osobiste, ponieważ według niej ma on prawny obowiązek ochrony jej danych osobowych, które gromadzi i zabezpiecza przed dostępem osób nieuprawnionych. Skarżąca wniosła o zbadanie, czy nie nastąpiło naruszenie przepisów ustawy o ochronie danych osobowych.

W przedmiotowym stanie faktycznym i prawnym Generalny Inspektor decyzją administracyjną odmówił uwzględnienia wniosku skarżącej[90]. Placówka Straży Granicznej i Oddział Straży Granicznej udostępniły dane osobowe skarżącej na żądanie sądu okręgowego na potrzeby toczącego się postępowania. Wskazać zatem należy, że przedmiotowe udostępnienie danych nastąpiło na podstawie art. 248 § 1 K.p.c., który stanowi, że 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.

Jednocześnie Generalny Inspektor wskazał, iż nie może oceniać celowości zbierania dowodów przez sąd. Postępowanie dowodowe w postępowaniu sądowym podlega ocenie w trybie instancyjnym na podstawie właściwych przepisów prawa. Mając na uwadze powyższe wskazane zostało, iż udostępnienie danych osobowych skarżącej jako niezbędne dla zrealizowania przez Placówkę Straży Granicznej oraz Oddział Straży Granicznej obowiązku wynikającego z przepisu prawa, znajduje oparcie w przesłance określonej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

[90] Decyzja GIODO z dnia 26 listopada 2013 r. DOLiS/DEC-1220/13/78666,78677,78690.

4) Organizacje społeczne

W roku sprawozdawczym 2013 r. wpłynęły do Biura GIODO również **63** skargi dotyczące **organizacji społecznych**.

Generalny Inspektor Ochrony Danych Osobowych decyzją z dnia 21 lutego 2013 r.[91] odmówił uwzględnienia wniosku w sprawie **ze skargi na przetwarzanie danych osobowych skarżącej przez stowarzyszenie**. Skarżąca w treści skargi wskazała, że prosi o przeprowadzenie postępowania administracyjnego, celem wyjaśnienia dlaczego jej dane osobowe zawarte w piśmie skierowanym do stowarzyszenia zostały publicznie odczytane w obecności osób zgromadzonych na szkoleniu na inspektora działającego na rzecz tego stowarzyszenia. Skarżąca podniosła, że stowarzyszenie jest organizacją, która powinna szanować ochronę prywatności zgodnie z przepisami ustawy o ochronie danych osobowych i nie powinna udostępniać jej danych osobowych, bez jej wiedzy i zgody osobom trzecim.

W treści decyzji organ do spraw ochrony danych osobowych wskazał, że w sprawie dopuszczalności przetwarzania informacji o imieniu i nazwisku skarżącej w kwestionowany przez nią sposób, skarżąca niezasadnie przyjmuje, że doszło do udostępnienia jej danych osobowych przez stowarzyszenie na rzecz osób trzecich. Z zebranego w sprawie materiału dowodowego wynikało, że z danymi osobowymi skarżącej zapoznali się wyłącznie członkowie stowarzyszenia uczestniczący w zamkniętym zebraniu. W związku z powyższym dane były przetwarzane jedynie przez administratora danych, czyli stowarzyszenie. Ponadto po stronie stowarzyszenia leżało rozpatrzenie skargi na związane z przedmiotem jej działalności działanie członka, co jest jego prawnie usprawiedliwionym celem. Na członkach stowarzyszenia ciążą bowiem pewne obowiązki wskazane w statucie, a prowadzenie działalności sprzecznej z postanowieniami tego statutu, zgodnie z jego § 15, może skutkować ustaniem członkowstwa. Dla dokonania oceny zasadności skargi niewątpliwie niezbędne było zapoznanie się przez osoby biorące udział w procesie jej rozpatrywania, z informacjami zawartymi w jej treści, a w konsekwencji tego również z informacjami stanowiącymi dane osobowe w rozumieniu ustawy, o ile takie znajdują się w skardze. Zaznaczyć jednocześnie należy, że Generalny Inspektor nie mógł kwestionować przyjętego przez stowarzyszenie trybu rozpatrzenia skargi (na zebraniu członków i w obecności osoby, której skarga dotyczyła). W ocenie Generalnego Inspektora nie można również uznać, że zaistniała okoliczność

[91] Decyzja GIODO z dnia 21 lutego 2013 r. DOLiS/DEC-200/13/10990,10994.

wyłączająca dopuszczalność przetwarzania danych, o której mowa w art. 23 ust. 1 pkt 5 ustawy, tj., że doszło do naruszenia praw i wolności skarżącej. Informacja o imieniu i nazwisku skarżącej była zawarta w treści rozpatrywanej skargi w kontekście działalności skarżącej w stowarzyszeniu, tj. działalności o charakterze publicznym, nie zaś w kontekście jej życia prywatnego. Skarżąca biorąc udział w działalności organizacji zajmujących się ochroną zwierząt musi liczyć się z tym, że jej dane osobowe w zakresie imienia i nazwiska, będą przetwarzane przez osoby obracające się w tym środowisku.

5) Banki i inne instytucje finansowe

W omawianym roku sprawozdawczym wpłynęło **247** skarg, w których zakwestionowano legalność działań **banków i innych instytucji finansowych.**

Wykres 15: ***Zestawienie porównawcze liczby skarg dotyczących sektora banków i innych instytucji finansowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2013.***

W jednej z takich spraw skarżący podniósł, że otrzymuje on od banku propozycję zawarcia umów na produkty bankowe, które dostępne są aktualnie w ofercie, pomimo, że nigdy nie był on klientem banku. Ponadto skarżący zarzucił, iż bank wszedł w posiadanie jego danych osobowych w inny sposób niż od niego, a co za tym idzie w żaden sposób nie spełnił wobec niego obowiązku informacyjnego wynikającego z ustawy. Dodał, że nie

wyrażał też zgody na przetwarzanie jego danych przez bank w celach marketingowych, nie posiada wiedzy, by bank udostępniał jego dane innym podmiotom.

Po przeprowadzeniu postępowania administracyjnego w niniejszej sprawie Generalny Inspektor Ochrony Danych Osobowych ustalił, iż skarżący w 2008 r. zawarł umowę o przyznanie limitu kredytowego z bankiem, który w wyniku połączenia w 2010 r. został w całości przejęty przez bank, którego dotyczy skarga. W tym stanie faktycznym Generalny Inspektor wydał decyzję nakazującą bankowi spełnienie wobec skarżącego obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych, poprzez poinformowanie go: a) adresie swojej siedziby i pełnej nazwie, b) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, c) źródle danych, d) prawie dostępu do treści swoich danych oraz ich poprawiania, e) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 ustawy o ochronie danych osobowych, f) uprawnieniach wynikających z art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych, zaś w pozostałym zakresie odmówił uwzględnienia wniosku[92].

W treści ww. decyzji organ podniósł, iż bank nabył całą bazę danych osobowych, w tym również i dane skarżącego, stworzoną przez inny bank w trybie art. 492 § 1 pkt 1 ustawy z dnia 15 września 2000 r. Kodeksu spółek handlowych (Dz. U. z 2013 r. poz. 1030), zwanej dalej K.s.h. W ten sposób bank wstąpił w prawa i obowiązki poprzedniego administratora danych, więc co do zasady nie „zbierał" danych w ścisłym znaczeniu, o którym mowa w art. 25 ust. 1 ustawy. Niemniej jednak nie budziło wątpliwości organu, że bank ze swej perspektywy pozyskał zupełnie nowe dane osobowe, których wcześniej nie przetwarzał i pozyskał je nie od osób, których dane dotyczą, lecz od innego administratora. W ocenie Generalnego Inspektora pojęcie „zbierania danych" w rozumieniu art. 25 ustawy, obejmuje wszystkie przypadki, w których administrator uzyskuje nowe, ze swej perspektywy, dane osobowe. Taką szczególną formą zbierania danych osobowych jest nabywanie zbiorów danych, które zostały stworzone przez inne podmioty. W takim przypadku administrator nie zbiera pojedynczych danych osobowych, lecz rozpoczyna przetwarzanie całego zbioru danych, w skład którego wchodzą dane osobowe zebrane przez inne podmioty. Przyjęcie liberalnej koncepcji o tym, że hipotezy art. 25 ustawy nie realizuje pozyskiwanie danych od innego administratora danych, gdyż dotyczy tylko „pierwotnego" pozyskiwania danych,

[92] Decyzja GIODO z dnia 4 października 2013 r. DOLiS/DEC-1073/13/64887,64889.

mogłoby prowadzić do sytuacji, w której podmiot danych nie miałby wiedzy co do tego, kto, na jakiej podstawie, w jakim zakresie i w jakim celu przetwarza dotyczące go dane, a co za tym idzie, nie miałby także możliwości wykonywania uprawnień przewidzianych w art. 32 ustawy, stąd też Generalny Inspektor Ochrony Danych Osobowych z taką liberalną koncepcją się nie zgadza.

W związku z powyższym, bank bezpośrednio po utrwaleniu zebranych danych skarżącego (danych przejętych od innego banku) winien spełnić wobec skarżącego obowiązek informacyjny, o którym mowa w art. 25 ust. 1 ustawy. W sprawie nie zachodziły okoliczności z art. 25 ust. 2 ustawy wyłączające przedmiotowy obowiązek, a z materiału dowodowego sprawy nie wynikało, by obowiązek ten został spełniony. Powyższe niedopełnienie obowiązku informacyjnego uniemożliwiło w szczególności skarżącemu, który nie godził się na otrzymywanie informacji o charakterze marketingowym, odwołanie złożonej zgody, czy wniesienie sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy. Prawidłowe spełnienie przez bank obowiązku informacyjnego z art. 25 ust. 1 ustawy miało na celu umożliwienie skarżącemu skorzystania z przysługujących mu uprawnień.

W 2013 r. organ do spraw ochrony danych osobowych wydał również **decyzję w sprawie nakazania bankowi spełnienia obowiązku informacyjnego z art. 33 ustawy usunięcia danych osobowych skarżącej przez bank i spółkę prowadzącą działalność windykacyjną[93].** W toku przeprowadzonych w sprawie czynności wyjaśniających, organ ochrony danych osobowych ustalił, iż bank nie przetwarzał, a w szczególności nie udostępnił na rzecz spółki, danych osobowych skarżącej. Bank przetwarzał natomiast dane osobowe osoby noszącej tożsame ze skarżącą imię i nazwisko, które to dane udostępnił na rzecz spółki w związku z zawartą umową cesji. Dane, które udostępnione zostały na rzecz spółki przez bank, nie dotyczyły zatem skarżącej, tylko innej osoby o zbieżnym ze skarżącą nazwisku.

W szczególności zaakcentowania wymaga, iż adres zamieszkania osoby o takim samym imieniu i nazwisku jak skarżąca, który bank udostępnił na rzecz spółki, był inny niż adres zamieszkania skarżącej, na który to adres zamieszkania skarżącej spółka kierowała korespondencję wzywającą do uregulowania długu. Kierowanie do skarżącej przez spółkę pism wzywających do uregulowania długu, które to pisma zaadresowane były do innej osoby o tym samym imieniu i nazwisku na adres skarżącej, wiązało się z dokonaniem przez ten

[93] Decyzja z dnia 7 marca 2013 r. DOLiS/DEC-267/13/14662,14665,14666.

podmiot błędnych ustaleń, co do osoby dłużnika w toku prowadzonych czynności windykacyjnych. Analiza przez spółkę zarzutów skarżącej dotyczących uznawania ją przez ten podmiot za swojego dłużnika i kierowania do niej korespondencji w tym przedmiocie doprowadziła jednak finalnie do usunięcia danych osobowych skarżącej przez spółkę. W ww. zakresie organ umorzył postępowanie w sprawie, zaś odnosząc się do pierwszego z zarzutów sformułowanych w skardze Generalny Inspektor nakazał bankowi spełnienie obowiązku informacyjnego poprzez udzielenie skarżącej informacji zawartych w art. 32 ust. 1 pkt 1-5a ustawy. Skarżąca, otrzymując do spółki wezwanie do uregulowania długu oraz informację o pozyskaniu, w celu wyegzekwowania ww. należności, jej danych osobowych od banku, powzięła informację o przetwarzaniu jej danych osobowych przez obydwa podmioty. Pomimo zatem, iż przeprowadzone postępowanie dowodowe wykazało, że dane osobowe skarżącej nie są i nigdy nie były przez bank przetwarzane, uzasadnionym i w pełni zrozumiałym było podjęcie przez skarżącą kroków zmierzających do uzyskania informacji o podstawie prawnej i celu przetwarzania jej danych osobowych przez bank. Jak bowiem wskazała skarżąca, nigdy nie była związana z bankiem stosunkiem cywilnoprawnym, a wystosowanie przez nią żądania zrealizowania wobec niej obowiązku informacyjnego z art. 33. ustawy miało na celu podjęcie ochrony jej interesów i stanowiło realizację przyznanych ustawą uprawnień. W ocenie Generalnego Inspektora pismo banku skierowane do skarżącej nie stanowiło odpowiedzi na rzeczone zapytanie skarżącej. Organ pokreślił, że spełnienie przez bank obowiązku informacyjnego powinno być poprzedzone rzetelną analizą tożsamości osoby występującej o realizację swoich uprawnień, która to analiza powinna się odbyć w oparciu o przetwarzane przez bank informacje dotyczące wnioskodawcy. Bank przy weryfikacji tożsamości wnioskodawcy zaniedbał obowiązki administratora danych rezygnując chociażby z wystąpienia do skarżącej o podanie numeru paszportu, co w niniejszej sprawie pozwoliłoby na poczynienie ustalenia, iż jej dane osobowe nie są przez bank przetwarzane.

W wyniku powyższego zaniedbania udostępniono skarżącej informacje objęte tajemnicą bankową i jednocześnie nie zrealizowano wobec niej obowiązku informacyjnego odnoszącego się do jej danych osobowych. Powyższe stało się dla Generalnego Inspektora Ochrony Danych Osobowych przyczynkiem do skierowania do banku sygnalizacji w rzeczonym przedmiocie[94].

[94] Pismo GIODO z dnia 7 marca 2013 r. DOLiS-440-134/12/MB/I/14658/13.

Duża część spośród skarg dotyczących przetwarzania danych osobowych przez banki dotyczyła kwestii ich **udostępniania na rzecz Biura Informacji Kredytowej S.A. (BIK).** Do Biura GIODO wpłynęła skarga na bank, który w związku z wnioskiem o kredyt konsumencki, niemający związku z prowadzoną przez skarżącego działalnością gospodarczą, udostępnił na rzecz BIK S.A. jego dane osobowe.

Bank - oprócz publicznie dostępnych danych identyfikujących przedsiębiorcę - przekazał również inne dane osobowe, jak numer PESEL, numer dowodu osobistego, datę urodzenia, numer wniosku kredytowego, wysokość wnioskowanego kredytu, wysokość raty kredytowej. Skarżący podkreślił, że nie udzielił bankowi zgody na przetwarzanie jego danych osobowych ani na ich przekazywanie do BIK. W związku z powyższym skarżący zarzucił bankowi naruszenie art. 23 ust. 1 w zw. z art. 24 ust. 1, art. 32 ust. 1 pkt 4, art. 36-39a, art. 40 ustawy o ochronie danych osobowych. Po przeprowadzeniu postępowania wyjaśniającego w sprawie organ do spraw ochrony danych osobowych ustalił, iż BIK pozyskał dane osobowe skarżącego w związku z zapytaniem kredytowym skierowanym przez poprzednika prawnego banku w stycznia 2006 r. w zakresie: imienia, nazwiska, płci, daty urodzenia, obywatelstwa, numeru PESEL, serii i numeru dokumentu tożsamości oraz warunków finansowych kredytu. Pozyskanie tych danych nastąpiło poprzez złożenie zapytania do BIK w związku z wnioskiem kredytowym z 2006 r. Zgodnie z regulaminem Biura Informacji Kredytowej zapytania są przechowywane w Bazie Informacji o Zapytaniach (BIOZ) przez okres nie dłuższy niż 2 lata.

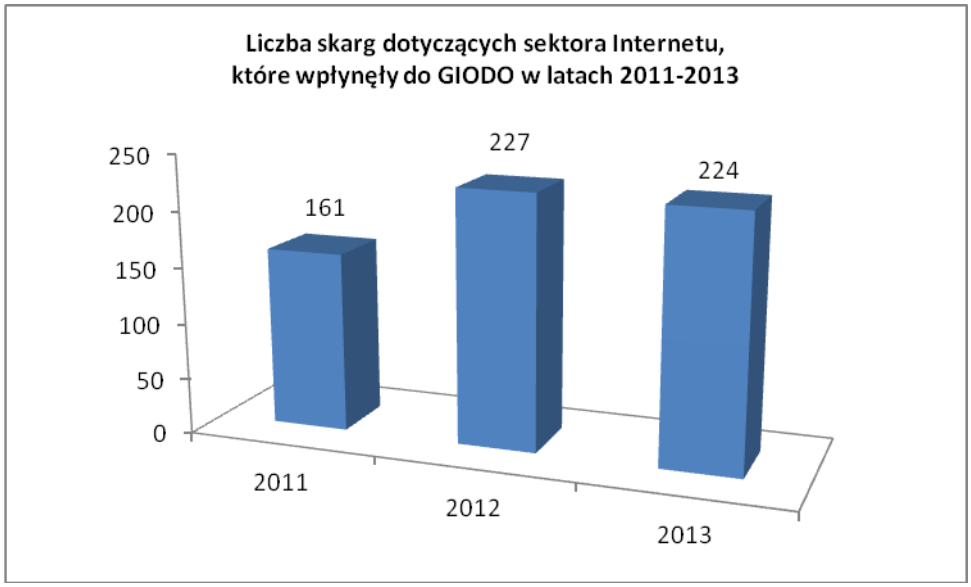
W związku z upływem tego okresu BIK - na moment wydania decyzji -przetwarzał dane osobowe skarżącego w celu rozpatrywania jego reklamacji i nie udostępniał ich bankom w raportach kredytowych. W związku z powyższym Generalny Inspektor decyzją administracyjną nakazał Biuru Informacji Kredytowej usunięcie danych osobowych skarżącego, zaś w pozostałym zakresie odmówił uwzględnienia wniosku[95]. W treści ww. decyzji organ m.in. wskazał, że zgodnie z art. 5 ustawy, 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. Tym samym, w ocenie Generalnego Inspektora, BIK S.A. nie legitymował się podstawą prawną do przetwarzania danych osobowych skarżącego pozyskanych od banku w jakimkolwiek innym celu, niż wskazane w ustawie Prawo bankowe.

[95] Decyzja GIODO z dnia 2 października 2013 r. DOLiS/DEC-1065/13/64164,64185,64191

Dlatego też nie sposób zgodzić się z tezą przedstawioną przez ten podmiot w złożonych wyjaśnieniach, że przetwarzanie przez niego danych osobowych może odbywać się dla realizacji innego celu realizowanego przez administratora danych (tu: BIK S.A.), którym w niniejszej sprawie jest potrzeba realizowania ewentualnych reklamacji skarżącego. Katalog przesłanek, w oparciu o które BIK może przetwarzać dane osobowe pozyskane od banków został określony enumeratywnie w przepisach Prawa bankowego. Również cele, dla których te dane mogą być przetwarzane, wynikają wprost z przepisów ww. ustawy. BIK nie wykazał podstaw prawnych dla przetwarzania danych skarżącego w tzw. celach „ewentualnych reklamacji". Przetwarzanie danych w tych celach może dodatkowo zostać uznane za przetwarzanie „na zapas", co narusza zasady adekwatności i celowości wyrażone w art. 26 ust. 1 ustawy o ochronie danych osobowych.

6) Internet

W 2013 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęły **224** skargi dotyczące **Internetu**, co jest porównywalne z minionym okresem sprawozdawczym, w którym skarg tych było 227.



Wykres 16: ***Zestawienie porównawcze liczby skarg dotyczących sektora Internetu, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2011-2013.***

Jedno z postępowań dotyczyło **skargi na zamieszczanie na stronie internetowej opinii dotyczących wykonywanego przez skarżącego zawodu wraz z podaniem adresu prowadzenia przez niego działalności gospodarczej.** Skarżący wniósł do spółki prowadzącej portal internetowy o usunięcie jego danych, ta zaś odmówiła dokonania ww. czynności. Ponadto skarżący podniósł, iż spółka przetwarza jego dane osobowe w swojej działalności komercyjnej. Po przeprowadzeniu postępowania wyjaśniającego w niniejszej sprawie Generalny Inspektor Ochrony Danych Osobowych odmówił uwzględnienia wniosku[96], a po rozpatrzeniu wniosku o ponowne rozpatrzenie sprawy utrzymał ww. decyzję w mocy[97].

W decyzji organ do spraw ochrony danych osobowych podkreślił, że z regulaminu korzystania z serwisu wynika, iż spółka świadczy usługi drogą elektroniczną na rzecz użytkowników ww. serwisu internetowego, polegające na umożliwieniu użytkownikom wymiany informacji, komentarzy i opinii na temat wykonywanego przez skarżącego zawodu. Jednocześnie z postanowień regulaminu wynika, iż ww. podmiot decyduje o zamieszczeniu na stronie internetowej bądź też usunięciu z niej informacji, komentarzy lub opinii użytkowników.

Generalny Inspektor zwrócił uwagę na brzmienie art. 23 ust. 1 pkt 5 ustawy, zgodnie z którym przetwarzanie danych osobowych przez administratora nie może naruszać praw i wolności osoby, której dane dotyczą. W ocenie Generalnego Inspektora w analizowanej sprawie do takiego naruszenia nie doszło. Przetwarzanie danych osobowych przez administratora nie może zatem naruszać prawa do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (art. 47 Konstytucji).

Mając zatem na uwadze, że dane osobowe skarżącego udostępniane na ww. stronie internetowej dotyczą wyłącznie życia zawodowego skarżącego, nie sposób było uznać, że doszło do naruszenia jego prawa do ochrony życia prywatnego, rodzinnego czy też prawa do decydowania o swoim życiu osobistym. Co więcej, zawód wykonywany przez skarżącego uznawany był za zawód zaufania publicznego, którego wykonywanie jest istotne z punktu widzenia interesu publicznego. Ze względu na specyfikę wykonywanego zawodu osoba taka musi liczyć się z tym, iż jego dane osobowe podlegają słabszej ochronie. Nie ulega bowiem

[96] Decyzja GIODO z dnia 21 lutego 2013 r. DOLiS/DEC-201/13/10944,10946,10947.
[97] Decyzja GIODO z dnia 19 lipca 2013 r. DOLiS/DEC-777/13/47061,47062.

wątpliwości, że świadczona przez skarżącego praca, w szczególności sposób jej wykonywania i uzyskane efekty, podlegają społecznej kontroli.

Natomiast serwis internetowy umożliwiający użytkownikom zamieszczanie opinii i komentarzy dotyczących tego zawodu jest jednym z narzędzi, za pomocą którego osoby korzystające z usług takich osób mogą wykonywać tę społeczną kontrolę.

W innej sprawie Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie administracyjne w sprawie **skargi na umieszczenie danych osobowych skarżącego bez jego zgody w dwóch serwisach internetowych**. Pełnomocnik skarżącego nadmienił, że w oparciu o treść art. 32 ust 1 pkt 6 ustawy o ochronie danych osobowych, skierował korespondencję do administratora serwisów z żądaniem usunięcia danych osobowych skarżącego, zaś ten odmówił spełnienia żądania. W związku z powyższym skarżący wniósł o usunięcie jego danych osobowych umieszczonych w ww. portalach.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie, Generalny Inspektor w drodze decyzji administracyjnej nakazał administratorowi serwisów internetowych wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego poprzez usunięcie jego danych osobowych w zakresie imienia i nazwiska z jednego serwisu internetowego, zaś w pozostałym zakresie umorzył postępowanie[98].

W ocenie Generalnego Inspektora imię i nazwisko skarżącego w połączeniu z dalszymi, wzmacniającymi stopień identyfikacji informacjami na jego temat zamieszczonymi w jednym z zaskarżonych serwisów internetowych, pozwalają na jednoznaczną identyfikację tej osoby, a zatem informacje te stanowią dane osobowe. Analiza treści postu zacytowanego w serwisie nakazuje uznać, iż autor tego postu bez problemu zidentyfikował skarżącego na podstawie informacji zawartych w innym poście zacytowanym w powyższym serwisie, tak więc wnioskować należy, iż treść całokształtu zawartych w ww. serwisie internetowym informacji na temat skarżącego, umożliwia określenie jego tożsamości bez nadmiernych kosztów, czasu lub działań.

GIODO uznał także , że treści i informacje zawarte w serwisie internetowym wskazują, że nie jest on *stricte* serwisem o charakterze niezarobkowym, który służy jego użytkownikom do wyrażania opinii o działalności firm i instytucji oraz osób prowadzących działalność

[98] Decyzja GIODO z dnia 4 października 2013 r. DOLiS/DEC-1072/13/64881,64884.

gospodarczą, bowiem zamieszczone są tam również treści i informacje o charakterze komercyjnym, tj. banery reklamowe i odnośniki do innych stron komercyjnych.

W kontekście powyższego Generalny Inspektor uznał, iż serwis internetowy mimo, że był zarejestrowany na osobę prywatną, nie jest związany z prowadzoną przez osobę skarżoną działalnością gospodarczą. Zgodnie z art. 3 ust. 2 pkt 2 ustawy, ustawę stosuje się również do osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych - które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Analiza materiału dowodowego zgromadzonego w sprawie, w kontekście cytowanego art. 3 ust. 2 pkt 2, nakazała uznać, że do niniejszego przypadku przetwarzania danych osobowych znajdują zastosowanie postanowienia ustawy o ochronie danych osobowych. Niewątpliwie bowiem działalność administratora prowadzącego serwis internetowy miała charakter zarobkowy.

Z ustaleń wynikało także, że podmiot ten był abonentem serwisu oraz usługodawcą w rozumieniu art. 2 pkt 6 ustawy o świadczeniu usług drogą elektroniczną. Co więcej, nie uzyskał zgody skarżącego na przetwarzanie jego danych osobowych, a jednocześnie żaden przepis prawa nie upoważniał go do przetwarzania danych skarżącego celem zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Przetwarzanie danych osobowych skarżącego nie było też konieczne do realizacji umowy, której stroną byłby skarżący ani też nie było niezbędne do podjęcia działań zmierzających do zawarcia takiej umowy. Nie wykonywał też określonych prawem zadań realizowanych dla dobra publicznego, z czym wiązałaby się konieczność przetwarzania danych skarżącego. Ponadto udostępnienie danych osobowych skarżącego nie było niezbędne dla wypełnienia prawnie usprawiedliwionego celu, a przy tym naruszało prawa i wolności skarżącego.

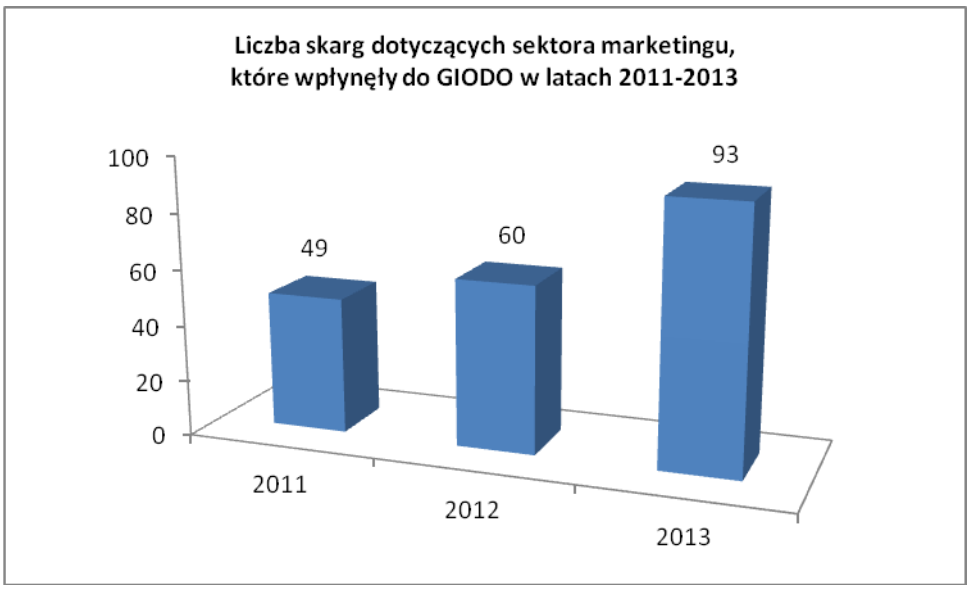
W niniejszej sprawie podmiot skarżony nie uzyskał od skarżącego zgody na przetwarzanie jego danych, a jednocześnie nie zachodziła żadna z przesłanek określonych w art. 23 ust. 1 pkt 2-5 ustawy, usprawiedliwiających przetwarzanie danych osobowych skarżącego w kwestionowany przez niego sposób. Ponadto nie podjęto działań zmierzających

do usunięcia stanu naruszenia prawa na szkodę skarżącego, w tym także po wniesieniu przez pełnomocnika skarżącego wniosku o usunięcie jego danych.

W ocenie Generalnego Inspektora w przedmiotowej sprawie należało uznać, iż dane osobowe skarżącego były przetwarzane w serwisie internetowym bez podstawy prawnej i dlatego koniecznie było, na podstawie art. 18 ust. 1 pkt 6 ustawy, nakazanie wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego. Odnosząc się zaś do przetwarzania danych osobowych skarżącego w drugim z serwisów internetowych wskazać należy, iż na dzień wydania decyzji serwis ten był niedostępny i tym samym dane osobowe skarżącego nie były na nim upubliczniane. Zatem w opinii GIODO postępowanie to stało się bezprzedmiotowe i zostało umorzone.

7) Marketing

W analizowanym okresie do GIODO wpłynęły **93** skargi na podmioty działające w sektorze **marketingu.** Dla porównania w 2012 r. wpłynęło 60 skarg dotyczących tego obszaru.



Wykres 17: ***Zestawienie porównawcze liczby skarg dotyczących sektora marketingu, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2011-2013.***

Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie w sprawie **skargi na przetwarzanie danych osobowych skarżącego przez jednego z operatorów telekomunikacyjnych w celach marketingowych.** Skarżący poinformował, iż zadzwoniła do niego przedstawicielka firmy jednej ze spółek działającej w sektorze bankowości proponując – w ramach współpracy z siecią telekomunikacyjną – skorzystanie z oferty karty kredytowej oraz że jego dane osobowe, pomimo wyraźnego braku zgody, zostały przekazane zewnętrznemu partnerowi tej sieci. Poinformował także, że zadzwoniła do niego konsultantka departamentu sprzedaży spółki proponując nowy telefon i usługę promocyjną, oraz że mimo wielokrotnych interwencji otrzymywał sms-y reklamowe.

Po przeprowadzeniu postępowania administracyjnego w niniejszej sprawie Generalny Inspektor w drodze decyzji administracyjnej nakazał spółce usunięcie uchybień w procesie przetwarzania danych osobowych poprzez zaprzestanie ich przetwarzania w celach marketingowych[99].

W ocenie Generalnego Inspektora w procesie przetwarzania danych osobowych skarżącego przez spółkę doszło do wielokrotnych uchybień polegających na przetwarzaniu jego danych osobowych w celach marketingowych pomimo niedopuszczalności takich operacji. Zaznaczyć jednocześnie należy, że z uwagi na brak możliwości jednoznacznego ustalenia, czy skarżący po wycofaniu zgody na otrzymywanie informacji handlowej za pomocą środków komunikacji elektronicznej, wyrażał zgody na ww. działanie w konkursach organizowanych przez spółkę (co jest okolicznością sporną pomiędzy stronami), nie jest możliwe dokonanie oceny czy z naruszeniem przepisów o ochronie danych osobowych odbywało się otrzymywanie przez niego sms-ów w 2009 r.

Dla rozstrzygnięcia w niniejszej sprawie istotne znaczenie miały jednak inne okoliczności. Zdaniem Generalnego Inspektora spółka dopuściła się przetwarzania danych osobowych skarżącego w celach marketingowych, pomimo wniesionego przez niego sprzeciwu wobec takich działań. Skarżący w skierowanej do spółki korespondencji e-mail wskazał jednoznacznie, że nie życzy sobie otrzymywać żadnych materiałów promocyjnych i ofert marketingowych. Był to więc sprzeciw wobec przetwarzania danych w celach marketingowych. W ocenie Generalnego Inspektora nie było dopuszczalne przetwarzanie

[99] Decyzja GIODO z dnia 28 maja 2013 r. DOLiS/DEC-585/13/33387,33394.

przez spółkę danych osobowych skarżącego w tych celach w oparciu o przesłankę określoną w art. 23 ust. 1 pkt 5 ustawy w późniejszym terminie, zarówno przez samą spółkę, jak i działającą na jej rzecz wskutek umowy powierzenia inną spółkę. Podkreślić należy, że mimo, iż skarżący swój sprzeciw ponowił, spółka dopiero po upływie wielu miesięcy uwzględniła żądanie skarżącego jako sprzeciw, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Zdaniem Generalnego Inspektora naruszyło to nałożoną na nią jako administratora danych przez art. 26 ust. 1 pkt 1 ustawy, powinność dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienia, aby dane te były przetwarzane zgodnie z prawem. Zasadnicze znaczenie dla rozstrzygnięcia sprawy miał jednak fakt, że spółka, wbrew przekazanej Generalnemu Inspektorowi informacji o fakcie zaprzestania przetwarzania danych osobowych skarżącego w celach marketingowych, nie zaprzestała tego działania. Przetwarzanie zaś w celach marketingowych danych osobowych byłego klienta, który wycofał zgodę na otrzymywanie informacji handlowych za pomocą środków komunikacji elektronicznej, wniósł sprzeciw wobec przetwarzania danych osobowych w celach marketingowych oraz nie wyraził zgody na przetwarzanie danych osobowych dla celów marketingowych po zakończeniu realizacji umowy, niewątpliwie nie znajduje oparcia w przepisach ustawy. Wobec stwierdzenia tego uchybienia zasadne było wydanie decyzji nakazującej spółce zaprzestanie przetwarzania danych osobowych skarżącego w celach marketingowych.

W treści innej skargi dotyczącej przetwarzania danych osobowych w celach marketingowych, skarżąca wskazała, że zamawiając nowy samochód w treści umowy sprzedaży **nie wyraziła zgody na przetwarzanie jej danych osobowych w celach marketingowych.** Pomimo powyższego do skarżącej skierowano szereg korespondencji o charakterze marketingowym. Skarżąca skierowała do spółki sprzeciw wobec takiego przetwarzania jej danych osobowych. W odpowiedzi spółka wskazała, że ww. oferta marketingowa została skierowana do skarżącej omyłkowo, a także potwierdziła, że odnotowała sprzeciw skarżącej wobec przetwarzania jej danych osobowych w celach marketingowych. Jednak pomimo ww. korespondencji od spółki do skarżącej ponownie skierowano ofertę marketingową.

W związku z powyższym skarżąca wniosła do GIODO skargę na działanie spółki. Po przeprowadzeniu postępowania wyjaśniającego w niniejszej sprawie Generalny Inspektor

Ochrony Danych Osobowych decyzją administracyjną odmówił uwzględnienia wniosku skarżącej[100]. W niniejszej sprawie organ ustalił, że skarżąca zawierając umowę ze spółką nie wyraziła zgody na przetwarzanie jej danych osobowych, umieszczonych w tej umowie, przez spółkę, przez Sieć Autoryzowanych Partnerów spółki (Koncesjonariuszy i ich Agentów) oraz przez podmioty, które przetwarzałyby powyższe dane w imieniu i na rzecz spółki w celach marketingowych. Brak powyższej zgody nie został prawidłowo odnotowany z powodu błędu pracownika koncesjonariusza spółki, czyli z przyczyn leżących po stronie administratora danych osobowych. Dopiero w okresie późniejszym do systemu informatycznego spółki wprowadzona została informacja o braku zgody skarżącej na przetwarzanie jej danych osobowych w celach marketingowych, co powinno skutkować zaprzestaniem przetwarzania danych w ww. celu w przyszłości od tej daty, jednakże po tej dacie skarżąca otrzymała kolejną korespondencję marketingową spółki. Wprawdzie spółka wskazywała, że dysponowała inną przesłanką przetwarzania danych skarżącej, tj. art. 23 ust. 1 pkt 5 ustawy, niemniej jednak przesłanka ta nie znajdowała zastosowania w omawianej sprawie wobec wyrażonego przez skarżącą żądania nieprzetwarzania jej danych, złożonego w momencie ich pozyskania przez spółkę.

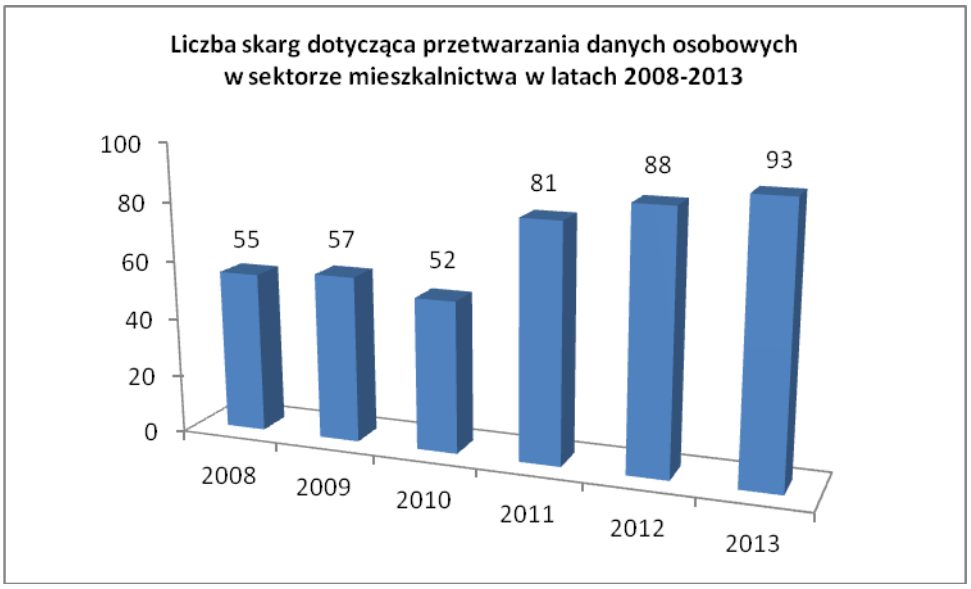
Podkreślenia wymaga, iż art. 23 ust. 1 pkt 5 uzasadnia przetwarzanie danych osobowych w celach marketingowych w czasie trwania umowy okresowej łączącej osobę, której dane dotyczą z administratorem danych, natomiast w przedmiotowej sprawie do przetwarzania danych skarżącej doszło po zrealizowaniu umowy, tak więc tylko zgoda osoby, której dane dotyczą może legalizować ten proces. W sytuacji, gdy spółka nie pozyskała zgody skarżącej na przetwarzanie jej danych osobowych w celach marketingowych po zrealizowaniu umowy, to prowadzenie działalności marketingowej odbywało się bez podstawy prawnej, a jednocześnie stanowiło przetwarzanie danych osobowych niezgodnie z celem, dla którego zostały one pozyskane, czyli dla realizacji umowy sprzedaży, co naraża spółkę na odpowiedzialność karną z art. 49 ustawy. Mimo iż poczynione w sprawie ustalenia faktyczne oraz prawne wskazywały, że w niniejszej sprawie niewątpliwie doszło do wykorzystania danych osobowych skarżącej z naruszeniem ww. zasad ustawy, brak było podstaw do zastosowania przepisu art. 18 ust. 1 ustawy.

[100] Decyzja GIODO z dnia 28 października 2013 r. DOLiS/DEC-1126/13/71003,71006.

Mając jednak na względzie uchybienia spółki w niniejszej sprawie Generalny Inspektor Ochrony Danych Osobowych skierował do tego podmiotu wystąpienia, w którym zasygnalizował o konieczności przestrzegania zasad przetwarzania danych osobowych[101].

8) Mieszkalnictwo

W 2013 roku do Biura GIODO wpłynęły **93 skargi** dotyczące zagadnień związanych z **mieszkalnictwem.** Dla porównania w roku 2012 r. wpłynęło 88 skarg dotyczących tego sektora.



Wykres 18: ***Zestawienie porównawcze liczby skarg dotyczących sektora mieszkalnictwa, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2013.***

W analizowanym okresie sprawozdawczym Generalny Inspektor prowadził postępowanie wyjaśniające **w sprawie dotyczącej udostępnienia danych osobowych przez spółdzielnię mieszkaniową poprzez umieszczenie na tablicy ogłoszeniowej, znajdującej się w holu jednej z nieruchomości należącej do spółdzielni, skargi, którą skarżąca skierowała do rady nadzorczej spółdzielni.** Skarżąca zwróciła się do spółdzielni z prośbą o usunięcie jej danych umieszczonych na ww. tablicy ogłoszeniowej, jednak spółdzielnia

[101] Pismo GIODO z dnia 28 października 2013 r. DOLiS-440-1129/12/PW/I/71014.

odmówiła. Ponadto, jak wskazała skarżąca, nie była to sytuacja jednorazowa, lecz powtarzała się kilkakrotnie.

W niniejszej sprawie Generalny Inspektor Ochrony Danych Osobowych decyzją odmówił uwzględnienia wniosku[102]. Uznał bowiem, że działanie rady nieruchomości – organu spółdzielni mieszkaniowej, polegające na udostępnianiu danych osobowych skarżącej na tablicy ogłoszeń, nie znalazło uzasadnienia w choćby jednej z przesłanek wskazanych w art. 23 ust. 1 ustawy, ani w przepisach prawa spółdzielczego, czy też ustawy o spółdzielniach mieszkaniowych. Przepisy ww. ustaw bowiem wskazują warunki w jakich osoby upoważnione mogą zapoznać się z danymi spółdzielców. Podkreślenia również wymaga fakt, że zakres danych i informacji udostępnianych członkom spółdzielni powinien być adekwatny do ich potrzeb związanych ze zgodnym z prawem celem udostępnienia.

W związku z powyższym organ uznał, iż faktycznie doszło do naruszenia przez spółdzielnię przepisów m.in. ustawy o ochronie danych osobowych, jednakże naruszenie to zostało usunięte poprzez zdjęcie - na polecenie prezesa zarządu spółdzielni - z tablicy ogłoszeń pism zawierających dane osobowe skarżącej. Podkreślenia wymaga, iż zarząd spółdzielni podjął czynności mające na celu niedopuszczenie do powstania kolejnej sytuacji naruszającej przepisy ustawy o ochronie danych. Zarząd poinformował członków rady nieruchomości, iż działania polegające na upublicznianiu danych osobowych zawartych w pismach stanowią naruszenie przepisów ww. ustawy. Pismo to stanowiło odpowiedź zarządu na pismo rady nieruchomości, w treści którego rada zadeklarowała, iż w dalszym ciągu będzie wywieszać w gablotach informacyjnych do wiadomości mieszkańców pisma skarżącej. Jednocześnie biorąc powyższe pod uwagę, Generalny Inspektor, działając w oparciu o art. 19a ustawy, skierował do spółdzielni wystąpienie[103] mające na celu zapewnienia przestrzegania przepisów ustawy o ochronie danych osobowych w zakresie przetwarzania danych członków spółdzielni. Upublicznienie bowiem przez spółdzielnię w holu nieruchomości pism zawierających dane osobowe skarżącej niewątpliwie wykraczało poza zakres uprawnień spółdzielni. Żaden bowiem przepis prawa, na podstawie którego działają spółdzielnie, nie daje jej prawa do takiego upublicznienia danych osobowych. Ponadto spółdzielnia jako administrator danych w ten sposób dopuszcza do zapoznania się z upublicznionymi informacjami również przez osoby, które nie są jej członkami ani lokatorami.

[102] Decyzja GIODO z dnia 24 maja 2013 r. DOLiS/DEC-581/13/32716,32762.
[103] Pismo GIODO z dnia 24 maja 2013 r. DOLiS-440-982/12/OS/I/32766.

Podobną decyzję – o odmowie uwzględnienia wniosku skarżącego[104] - Generalny Inspektor Ochrony Danych Osobowych podjął **w sprawie dotyczącej przetwarzania danych osobowych w zakresie imienia, nazwiska i adresu zamieszkania przez Regionalne Towarzystwo Budownictwa Społecznego, zarządcę wspólnoty mieszkaniowej**.

Skarżący poinformował organ do spraw ochrony danych osobowych, że członkowie wspólnoty otrzymali do rąk własnych pismo od zarządcy z załącznikiem, który zawierał jego dane osobowe. Skarżący wskazał, że w jego ocenie zarządca naruszył przepisy o ochronie danych osobowych, a także zakwestionował celowość udostępnienia przedmiotowych danych osobowych, oraz zwrócił się o sprawdzenie czy osoba roznosząca omawianą informację z jego danymi osobowymi członkom wspólnoty jest uprawniona do przetwarzania danych osobowych członków wspólnoty.

9) Oświata i szkolnictwo wyższe

W omawianym okresie do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **41** skarg na podmioty działające w sektorze **oświaty**.

GIODO prowadził czynności wyjaśniające w związku ze **skargą dotyczącą przetwarzania danych osobowych przez jeden z uniwersytetów (dawniej politechnikę).** Skarżący wskazał, że w związku z bezprawnym przechowywaniem w archiwach uniwersytetu, w teczkach osobowych absolwentów politechniki, kopii pisma 30 studentów oraz kopii pisma przewodniczącego samorządu studenckiego, w których zawarte były żądania odsunięcia go od zajęć dydaktycznych, wnosi o nakazanie ujawniania mu oryginałów tych dokumentów, a także usunięcia ich kopii ze wszystkich zbiorów uniwersytetu, ponieważ zawierają one nieprawdziwe informacje o jego osobie. Skarżący zwrócił się do Generalnego Inspektora o przywrócenie stanu zgodnego z prawem, tj. o usunięcie jego danych osobowych zawartych w treści wskazanych dokumentów, a w konsekwencji usunięcie tych dokumentów, nielegalnie przechowywanych w archiwach uniwersytetu w teczkach osobowych absolwentów politechniki.

Po przeprowadzeniu postępowania wyjaśniającego, Generalny Inspektor w drodze decyzji administracyjnej nakazał uniwersytetowi wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego poprzez usunięcie z teczek akt

[104] Decyzja GIODO z dnia 24 września 2013 r. DOLiS/DEC-1028/13/62205,62209,62211.

osobowych studentów danych osobowych skarżącego, utrwalonych w kopiach pisma studentów i pisma przewodniczącego samorządu studentów, zaś w pozostałym zakresie odmówił uwzględnienia wniosku[105]. Odnośnie przechowywania w teczkach akt osobowych studentów danych osobowych skarżącego utrwalonych w kopiach pism Generalny Inspektor stanął na stanowisku, iż działanie to nie znajduje uzasadnienia w żadnej z przesłanek określonych w art. 23 ust. 1 ustawy. Sposób prowadzenia przez uczelnie dokumentacji przebiegu studiów określają przepisy rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 14 września 2011 r. w sprawie dokumentacji przebiegu studiów (Dz. U. Nr 201, poz. 1188). To, jakie dokumenty mogą znajdować się w teczce akt osobowych studenta określa § 4 ust. 1 tego rozporządzenia. Pisma będące prośbą dotyczącą organizacji zajęć dydaktycznych, których współprowadzącym był skarżący, nie należą do dokumentów wskazanych w powyższym przepisie, wobec czego - zdaniem Generalnego Inspektora - brak było podstaw prawnych do przechowywania ich kopii w teczkach akt osobowych studentów będących autorami pism, a zatem również do przechowywania w ten sposób danych osobowych skarżącego utrwalonych w tych dokumentach.

Z uwagi zaś na niedopuszczalność takiego przechowywania danych, konieczne stało się rozstrzygnięcie sprawy w tym zakresie w sposób wskazany w art. 18 ust. 1 pkt 6 ustawy, poprzez usunięcie wnioskowanych przez skarżącego danych.

10) Służba zdrowia

W 2013 roku do Biura GIODO wpłynęło **48** skarg dotyczących **służby** z**drowia.**

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga, przekazana według właściwości przez dyrektora jednego z oddziałów wojewódzkich Narodowego Funduszu Zdrowia, na przetwarzanie danych osobowych skarżącej przez Narodowy Fundusz Zdrowia (NFZ). Skarżąca zakwestionowała legalność przetwarzania przez Fundusz jej danych osobowych, w szczególności informacji o niepełnosprawności. W związku z powyższym wniosła o usunięcie tych danych z bazy danych komputerowych i systemu informatycznego Funduszu. Po przeprowadzeniu postępowania wyjaśniającego Generalny Inspektor Ochrony Danych Osobowych odmówił uwzględnienia wniosku skarżącej[106].

[105] Decyzja GIODO z dnia 29 października 2013 r. (DOLiS/DEC-1135/13/71588,71665)
[106] Decyzja GIODO z dnia 11 lipca 2013 r. DOLiS/DEC-733/13/44122,44132.

W niniejszej sprawie skarżąca, w związku z wystąpieniem o skierowanie jej na leczenie uzdrowiskowe, załączyła do przedmiotowego wniosku orzeczenie o swojej niepełnosprawności. Potem zaś kwestionowała przetwarzanie przez NFZ ww. informacji i domagała się jej usunięcia z komputerowej bazy danych Funduszu. Z materiału dowodowego niniejszej sprawy wynikało, że kwestionowane przez skarżącą działania Funduszu związane z przetwarzaniem jej danych osobowych, w tym oceną zasadności skierowania skarżącej na leczenie uzdrowiskowe, zostały przeprowadzone zgodnie z przepisami szczególnymi odnoszącymi się do analizowanego zagadnienia. Zatem przetwarzanie szczególnie chronionych danych osobowych skarżącej pozostaje w zgodzie z powołanym wyżej przepisem art. 27 ust. 2 pkt 2 ustawy. Skarżąca, co do zasady, kwestionowała natomiast postawioną diagnozę lekarską, a nie obiektywne kategorie danych osobowych, jak np. imię czy nazwisko, które to dane mogłyby ewentualnie zostać wpisane w sposób błędny czy nieprawdziwy, i których prawdziwość mogłaby podlegać weryfikacji. Generalny Inspektor Ochrony Danych Osobowych nie jest zaś uprawniony, w świetle kompetencji przyznanych mu w art. 12 ustawy, do weryfikowania rozpoznania co do stanu zdrowia skarżącej, dokonanego przez właściwej specjalizacji lekarza. Nie jest bowiem władny ingerować w diagnozę lekarską, a co za tym idzie, nie jest uprawniony do nakazania usunięcia czy sprostowania kwestionowanych przez skarżącą danych na jej temat, bo to właśnie wiązałoby się z przedmiotową ingerencją. Generalny Inspektor Ochrony Danych Osobowych nie był więc właściwy w przedmiocie nakazania usunięcia informacji o diagnozie lekarskiej zawartej w dokumentacji medycznej prowadzonej w systemie papierowym. Jednocześnie organ ochrony danych osobowych ustalił, że informacja o diagnozie lekarskiej nie była przetwarzana w systemie elektronicznym.

Generalny Inspektor Ochrony Danych Osobowych prowadził również postępowanie administracyjne **w sprawie udostępnienia przez Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych informacji dotyczących stanu zdrowia skarżącej na rzecz spółki, w której skarżąca była zatrudniona, jak również niewypełnienia przez szpital w stosunku do niej obowiązku informacyjnego określonego w art. 24 ust. 1 ustawy oraz odnotowania w systemie informatycznym szpitala jako osoby dokonującej operacji na danych osobowych skarżącej podczas jej przyjęcia do szpitala innej osoby niż ta, która w rzeczywistości dokonywała tych operacji.** Skarżąca zażądała przywrócenia stanu zgodnego z prawem oraz zobligowania dyrekcji szpitala do przesłania jej byłemu pracodawcy

pisma jednoznacznie stwierdzającego, że wszedł w posiadanie informacji dotyczących jej stanu zdrowia nie będąc do tego uprawnionym i nie nastąpiło to na jej prośbę, czy wniosek, tylko bez jej zgody, a nawet wiedzy, z naruszeniem prawa i było samowolnym działaniem administracji szpitalnej, a winę ponosi wyłącznie szpital.

Po przeprowadzeniu postępowania wyjaśniającego organ do spraw ochrony danych osobowych w drodze decyzji administracyjnej nakazał szpitalowi usunięcie uchybień w procesie przetwarzania danych osobowych skarżącej w zakresie realizacji obowiązku o którym mowa w art. 24 ust. 1 ustawy, poprzez poinformowanie jej o: a) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych, b) prawie dostępu do treści swoich danych oraz ich poprawiania, c) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej; zaś w pozostałym zakresie odmówił uwzględnienia wniosku[107].

W ocenie Generalnego Inspektora przekazana spółce przez szpital informacja o przyjęciu skarżącej w celu leczenia szpitalnego była informacją o stanie zdrowia skarżącej. Na stan zdrowia skarżącej jednoznacznie wskazuje określony w zaświadczeniu cel przyjęcia jej do szpitala. Wobec tego dopuszczalność udostępnienia danych osobowych przez szpital należy oceniać na gruncie przepisów art. 27 ustawy o ochronie danych osobowych.

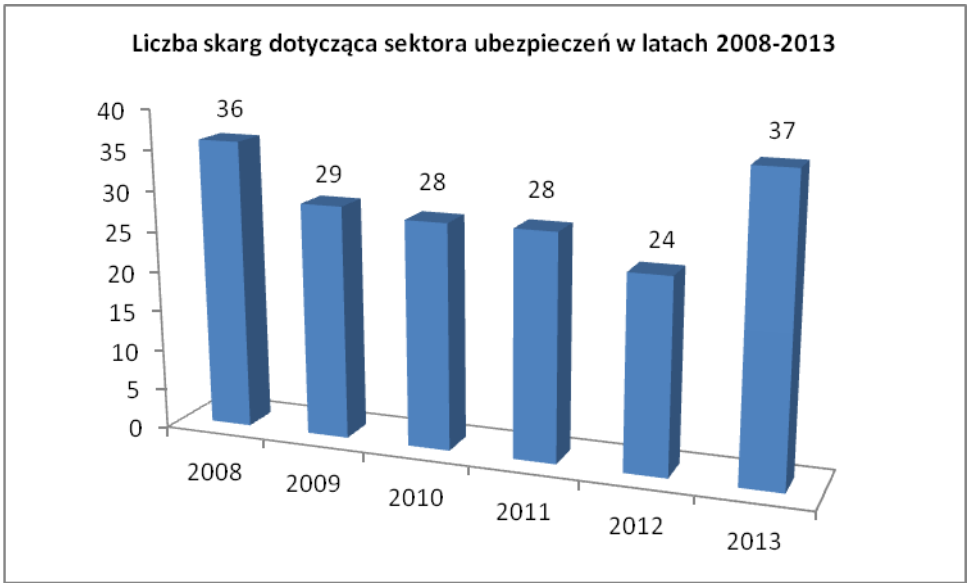
Zdaniem Generalnego Inspektora udostępnienie przez szpital informacji o stanie zdrowia skarżącej nie znalazło uzasadnienia w żadnej z przesłanek wskazanych w art. 27 ust. 2 ustawy, a w szczególności w przesłance określonej w powoływanym przez szpital, jako podstawa jego działania, art. 27 ust. 2 pkt 3 ustawy. Ponadto z materiału dowodowego zgromadzonego w sprawie wynikało, iż skarżąca w dniu przyjęcia do szpitala podpisała zgodę na hospitalizację. Generalny Inspektor podzielił stanowisko zajęte przez Rzecznika Praw Pacjenta, który w skierowanym do szpitala wystąpieniu stwierdził, że nie ma przesłanek wskazujących na fakt, iż skarżąca była niezdolna do wyrażania woli. Niezależnie od powyższego zauważyć należy, że skarżąca w chwili przyjęcia do szpitala nie pozostawała w stosunku pracy ze spółką. Zatem w chwili udostępnienia danych nie występowała wskazywana przez szpital potrzeba ochrony jej interesu, polegającego na ochronie jej stosunku pracy, a szpital udostępnił dane osobowe w oparciu o nieaktualną

[107] Decyzja GIODO z dnia 19 czerwca 2013 r. DOLiS/DEC-647/13/38538,38554,38558.

i niezweryfikowaną informację o zatrudnieniu skarżącej. W ocenie GIODO zebrany w sprawie materiał dowodowy wskazywał, iż szpital nie wypełnił w stosunku do skarżącej obowiązku określonego w art. 24 ust. 1 ustawy w zakresie, w jakim był obowiązany. Zatem zgodnie z art. 18 ust. 1 pkt 1 ustawy, zasadnym było nakazanie szpitalowi usunięcia uchybień w procesie przetwarzania danych osobowych skarżącej.

11) Ubezpieczenia społeczne, majątkowe i osobowe

W sektorze **ubezpieczeń społecznych, majątkowych i osobowych** można odnotować – w stosunku do poprzedniego roku sprawozdawczego - nieznaczny wzrost liczby skarg kierowanych do Generalnego Inspektora**.** W 2013 r. do Biura GIODO wpłynęło **37** skarg, zaś w poprzednim roku sprawozdawczym było ich 24. Niemniej jednak liczba wniesionych skarg na podmioty działające w tym sektorze od kilku lat utrzymuje się na wyrównanym poziomie, co pokazuje poniższy wykres.



Wykres 19: ***Zestawienie porównawcze liczby skarg na podmioty działające w sektorze ubezpieczeń społecznych, majątkowych i osobowych, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2013.***

W roku 2013 Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie wyjaśniające **w sprawie skargi na nieprawidłowości w procesie przetwarzania danych osobowych skarżącego przez Towarzystwo Ubezpieczeń (TU).**

Skarżący podniósł, iż Towarzystwo Ubezpieczeń nie spełniło wobec niego obowiązku informacyjnego, o którym mowa w art. 33 ust. 1 ustawy.

W dniu 6 grudnia 2012 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną[108], mocą której nakazał Funduszowi Inwestycyjnemu Towarzystwo Ubezpieczeń na Życie reprezentowanemu przez Towarzystwo Ubezpieczeń na Życie, wypełnienie obowiązku informacyjnego z art. 33 w zw. z art. 32 ust. 1 pkt 3 ustawy w stosunku do skarżącego, poprzez podanie mu w powszechnie zrozumiałej formie treści jego danych osobowych zawartych w wyciągach stanu konta na indywidualnym koncie jednostek uczestnictwa prowadzonym w ramach polisy, oraz wypełnienie obowiązku informacyjnego z art. 24 ustawy poprzez udzielenie mu informacji o prawie dostępu do treści swoich danych oraz ich poprawiania, natomiast w pozostałym zakresie odmówił uwzględnienia wniosku. Po ponownym rozpatrzeniu sprawy, na skutek złożenia przez Towarzystwo Ubezpieczeniowe wniosku o ponowne rozpatrzenie sprawy, organ dokonał ustaleń, że w zakresie dotyczącym nakazu sformułowanego w pkt 1 ww. decyzji z dnia 6 grudnia 2012 r. dotyczącego obowiązku informacyjnego określonego w art. 24 ustawy w zakresie poinformowania skarżącego o prawie dostępu do jego danych osobowych i prawie ich poprawiania, zgodzić należało się z Towarzystwem Ubezpieczeniowym, że sformułowanie nakazu było niezasadne, jednakże z innych względów niż podniesione w ww. wniosku o ponowne rozpatrzenie sprawy. Towarzystwo Ubezpieczeniowe zarzuciło bowiem, że w tym zakresie skarżący nie wystąpił do niego z odpowiednim wnioskiem o podanie informacji. Tymczasem spełnienie obowiązku z art. 24 ustawy nie jest uzależnione od wniosku osoby, której dane dotyczą. GIODO uznał zaś, że zgodnie z przepisami ustawy o ochronie danych osobowych administrator danych był obowiązany w momencie zbierania danych od osoby, której dane dotyczą, dopełnić obowiązku z art. 24 ustawy w zakresie określonym dyspozycją tego przepisu.

Ponadto organ do spraw ochrony danych osobowych uznał, iż wyjawienie stanu konta czy informacje o wyciągach stanu konta na indywidualnym koncie jednostek uczestnictwa prowadzonym w ramach polisy, względnie – jak to doprecyzował skarżący – informacje o wszelkich operacjach wykonywanych na tym koncie w trakcie trwania umowy ubezpieczenia zawartej ze skarżącym, która uległa rozwiązaniu (tj. o wszystkich operacjach wykonywanych przez cały okres obowiązywania tej umowy) nie były informacją o treści danych osobowych

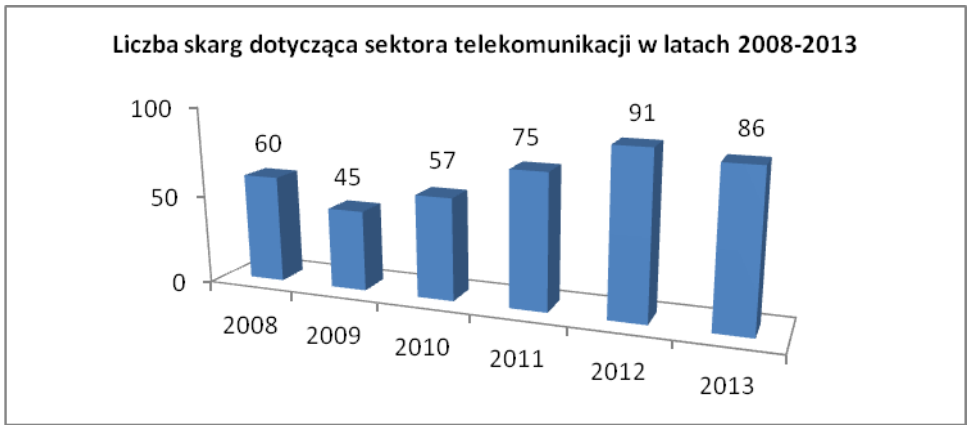
[108] Decyzja GIODO z dnia 6 grudnia 2012 r. DOLiS/DEC-1199/12/74277,74279.

przetwarzanych przez administratora danych osobowych, o której mowa w art. 32 ust. 1 pkt 3 ustawy *in fine*. Tym samym ww. informacje nie były informacjami, których udostępnienia można domagać się od administratora danych osobowych w trybie wniosku o spełnienie obowiązku informacyjnego, o którym mowa w art. 33 ust. 1 ustawy. Dokonana w zaskarżonej decyzji ocena uznająca informacje o wszelkich operacjach wykonywanych na indywidualnym koncie jednostek uczestnictwa za informacje podpadające pod dyspozycję przepisu w art. 32 ust. 1 pkt 3 ustawy *in fine* była błędna.

W związku z powyższym organ uznał, iż informacje o wszelkich operacjach wykonywanych na ww. koncie w trakcie trwania umowy ubezpieczenia nie mogą być uznane za dane osobowe w rozumieniu art. 6 ust. 1 ustawy, jako informacje odnoszące się do identyfikowanej osoby fizycznej, bowiem są to informacje finansowe dotyczące alokacji składek, o których mowa w umowie ubezpieczenia. Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej uchylił ww. decyzję z dnia 6 grudnia 2012 r. w odniesieniu do punktu I i w tym zakresie odmówił uwzględnienia wniosku skarżącego, zaś w pozostałym zakresie utrzymał zaskarżoną decyzję w mocy[109].

12) Telekomunikacja

W rozpatrywanych w 2013 r. sprawach dotyczących **telekomunikacji**, do Biura GIODO wpłynęło **86** skarg na podmioty tego sektora. Dla porównania w 2012 r. skarg tych było 91.



Wykres 20: ***Zestawienie porównawcze liczby skarg na podmioty działające w sektorze telekomunikacji, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2013.***

[109] Decyzja GIODO z dnia 15 listopada 2013 r. DOLiS/DEC-1186/13/75909,75916.

W analizowanym okresie Generalny Inspektor **prowadził postępowanie w przedmiocie naruszenia przetwarzania danych osobowych przez jedną ze spółek telekomunikacyjnych.** Skarżący podniósł, że jeden podmiot telekomunikacyjny udostępnił jego dane osobowe na rzecz innego podmiotu telekomunikacyjnego, co w rezultacie doprowadziło do zmiany operatora.

Po przeprowadzeniu postępowania w niniejszej sprawie organ do spraw ochrony danych osobowych ustalił, że do udostępnienia danych skarżącego doszło na skutek umowy zawartej przez skarżącego z operatorem. Proces zmiany operatora inicjuje operator alternatywny przekazując dotychczasowemu operatorowi zamówienie usługi hurtowego dostępu do sieci, a dotychczasowy operator jest zobowiązany do jego realizacji zgodnie z umową zawartą z danym operatorem. Spółka przedstawiła Generalnemu Inspektorowi umowę zamówienie na abonament telefoniczny na linii analogowej oraz oświadczenie o wypowiedzeniu umowy podpisane przez skarżącego. Bezsporny był zatem fakt, iż na podstawie zawartych zobowiązań pomiędzy operatorami telekomunikacyjnymi spółka przekazała dane osobowe skarżącego operatorowi alternatywnemu.

W związku z powyższym ww. przekazaniu nie sposób było odmówić walorów legalności. W rezultacie Generalny Inspektor Ochrony Danych Osobowych decyzją administracyjną odmówił uwzględnienia wniosku w niniejszej sprawie[110].

Organ do spraw ochrony danych osobowych przeprowadził również postępowanie w sprawie **skargi na przetwarzanie danych osobowych przez spółkę z branży telekomunikacyjnej.** Skarżący poinformował, że na jego prywatny numer dodzwoniła się osoba przedstawiająca się jako pracownik spółki, i która dysponowała informacjami dotyczącymi jego imienia i nazwiska, a także zakresu usług świadczonych na jego rzecz przez spółkę oraz wysokości opłat za te usługi. Skarżący weryfikując prawdziwość oferty skontaktował się ze spółką i uzyskał informację, że w tym dniu nie odnotowano żadnego połączenia do niego wykonywanego w imieniu spółki. W związku z powyższym skarżący nabrał przekonania, że jego dane osobowe zostały udostępnione przez spółkę osobom nieupoważnionym. Wskutek przeprowadzenia postępowania wyjaśniającego GIODO ustalił, iż połączenie telefoniczne wykonał pracownik spółki w jej imieniu, a nie podmiot, któremu spółka miała zdaniem skarżącego, udostępnić jego dane osobowe. Brak możliwości

[110] Decyzja GIODO z dnia 14 stycznia 2013 r. DOLiS/DEC-29/13/1981,1982.

potwierdzenia przez pracownika spółki podczas rozmowy telefonicznej, że przedmiotowa oferta telefoniczna pochodziła od spółki, spowodowane było jedynie brakiem odnotowania w systemie informatycznym faktu ww. połączenia z uwagi na niezainteresowanie skarżącego ofertą.

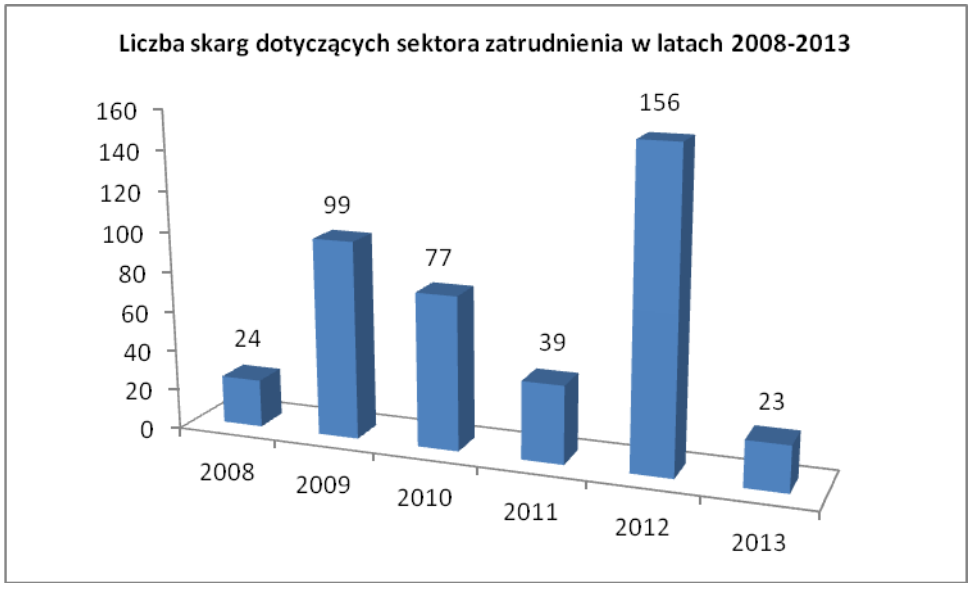
Z uwagi na fakt, iż Generalny Inspektor Ochrony Danych Osobowych nie dysponował żadnymi dowodami na potwierdzenie okoliczności przedstawionych w skardze, a skarżący oparł skargę jedynie na własnych podejrzeniach, organ odmówił uwzględnienia wniosku[111].

Duża liczba spośród skarg na podmioty sektora dotyczącego telekomunikacji, stanowiły **wnioski Komendanta Straży Miejskiej o nakazanie operatorom telekomunikacyjnym udostępnienia danych osobowych abonenta usług telekomunikacyjnych świadczonych przez spółkę, tj. użytkownika numeru telefonu w zakresie jego imienia, nazwiska oraz adresu zamieszkania.** W takich sytuacjach organ do spraw ochrony danych osobowych zwykle nakazywał operatorowi telekomunikacyjnemu udostępnienie żądanych przez Komendanta danych[112]. Organ do sprawy danych osobowych nakazywał udostępnienie w sposób, o którym mowa powyżej w oparciu o przepisy art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych w związku z art. 56 ust. 2 w zw. z art. 54 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia, art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach oraz art. 161 ust. 1 w zw. z art. 159 ust. 4 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

13) Zatrudnienie

W omawianym roku sprawozdawczym, do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęły **23** skargi, w których zakwestionowano legalność działań podmiotów z sektora **zatrudnienia**. W porównaniu z rokiem 2012, w którym odnotowano 156 skarg na podmioty działające w tym obszarze, oznacza to gwałtowny, prawie 7-krotny spadek liczby skarg.

[111] Decyzja GIODO z dnia 20 grudnia 2013 r. DOLiS/DEC-1313/13/85831,85840.
[112] Decyzje GIODO z dnia: 12 lutego 2013 r. - DOLiS/DEC-133/13/8353,8356; 18 lutego 2013 r. - DOLiS/DEC-168/13/9710,9714; 15 marca 2013 r. - DOLiS/DEC-301/13/16778,16782.



Wykres 21: ***Zestawienie porównawcze liczby skarg dotyczących sektora zatrudnienia, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2013.***

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga na przetwarzanie przez jeden z zespołów szkół ponadgimnazjalnych informacji o dochodach skarżącej (zatrudnionej w ww. placówce) oraz jej męża, pozyskane w związku ze składanymi przez nią wnioskami o świadczenia z funduszu świadczeń socjalnych, i informacji o stażu pracy skarżącej w celu sporządzenia dokumentu zatytułowanego „Dokonując oceny wyboru pracowników do zwolnienia pracodawca kieruje się następującymi kryteriami" oraz udostępnienie tych informacji na rzecz Międzyszkolnej Komisji NSZZ „Solidarność" Pracowników Oświaty i Wychowania oraz Związku Nauczycielstwa Polskiego. Skarżąca zarzuciła, że administrator danych ujawniając dane związkom zawodowym nie spełnił żadnej z przesłanek wynikających z art. 23 ust. 1 ustawy, a ponadto przygotowanie dokumentu było wyłączną inicjatywą pracodawcy, ponieważ sąd o takie dane nie pytał. W związku z koniecznością redukcji zatrudnienia spowodowaną niezatwierdzeniem jednego etatu pracownika obsługi, zespół uzgodnił z działającymi w nim związkami zawodowymi kryteria kolejności wypowiedzenia stosunku pracy z przyczyn niedotyczących pracownika. Do tych kryteriów należały m.in. staż pracy i kryterium socjalne (sytuacja osobista i materialna).

Po przeprowadzeniu postępowania wyjaśniającego w sprawie, Generalny Inspektor odmówił uwzględnienia wniosku[113] wskazując, że mimo, iż w jego ocenie udostępnienie na rzecz związków informacji o stażu pracy skarżącej i dochodach jej oraz jej męża, zawartych w dokumencie zatytułowanym „Dokonując oceny wyboru pracowników do zwolnienia pracodawca kieruje się następującymi kryteriami:", naruszyło przepisy o ochronie danych osobowych, to jednak z uwagi na nieodwracalność tego działania, nie jest możliwe wydanie przez Generalnego Inspektora decyzji nakazującej przywrócenie stanu zgodnego z prawem zgodnie z treścią art. 18 ust. 1 ustawy. Mając na względzie konieczność zapewnienia przez zespół należytego poziomu ochrony danych osobowych, Generalny Inspektor w odrębnym wystąpieniu zasygnalizował mu potrzebę uwzględnienia przepisów ustawy w dalszej działalności[114].

Ponadto Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie **w sprawie skargi na przetwarzanie danych osobowych przez spółkę (pracodawcę skarżącego) oraz przedsiębiorcę prowadzącego działalność gospodarczą.** Skarżący podniósł, iż przedsiębiorca działając w imieniu pracodawcy skarżącego zajmował się weryfikacją i zarządzaniem problemem absencji chorobowej pracowników. Skarżący poinformował, że w trakcie rozmowy przedsiębiorca zadawał pytania związane ze stanem zdrowia oraz tworzył protokół z takiego spotkania przedstawiany następnie kontrolowanemu pracownikowi do podpisu. W ocenie skarżącego spółka udostępniła jego dane osobie nieupoważnionej, przez co również naruszyła art. 36 ust. 1 ustawy. Generalny Inspektor Ochrony Danych Osobowych ustalił, iż spółkę i przedsiębiorcę łączyła umowa dotycząca przeprowadzenia przez przedsiębiorcę – na podstawie dostarczonych przez spółkę zwolnień lekarskich - kontroli prawidłowości wykorzystywania przez pracowników zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich. Spółka zobowiązała się do udostępnienia przedsiębiorcy wszelkich dokumentów i informacji niezbędnych do należytego wykonania umowy, a także upoważniła przedsiębiorcę do przetwarzania danych osobowych pracowników spółki w celu weryfikacji przedłożonych zwolnień chorobowych, na podstawie odrębnego upoważnienia stanowiącego załącznik do ww. umowy. Ponadto na dzień wydania decyzji przedsiębiorca nie przetwarzał już danych osobowych skarżącego. W związku z powyższym organ ds. ochrony danych osobowych w drodze decyzji

[113] Decyzja GIODO z dnia 8 października2013 r. DOLiS/DEC-1083/13/65758,65768,65777.
[114] Pismo GIODO z dnia 8 października 2013 r. DOLiS-440-794/12/LZ/I/ 65718/13.

administracyjnej umorzył postępowanie w sprawie przetwarzania danych osobowych skarżącego przez przedsiębiorcę, zaś w pozostałym zakresie odmówił uwzględnienia wniosku[115]. Jednocześnie Generalny Inspektor mając wątpliwości co do poprawności nadanych przez spółkę upoważnień do przetwarzania danych osobowych, wystosował do spółki wystąpienie, w którym zwrócił uwagę na uchybienia w tym zakresie[116].

W analizowanym okresie do organu ochrony danych osobowych wpłynęła **skarga dotycząca przetwarzania danych osobowych w zakresie wizerunku przez NZOZ (byłego pracodawcę skarżących) za pomocą stosowanego przez spółkę monitoringu.** Skarżące podniosły, iż monitoring w miejscu pracy obejmował m.in. rejestrację wizji nawet w szatni; rejestrację dźwięku, o czym skarżące nie zostały poinformowane.

Ponadto skarżące zauważyły, że zapisy monitoringu zostały udostępnione na rzecz sądu rejonowego, w którym toczyły się postępowania w sprawie rozwiązania z nimi umowy o pracę bez wypowiedzenia. Na płycie, przekazanej do sądu znajdowało się 17 plików o rozszerzeniu avi, z czego pliki o numerze 7 i 9 były nagrane z dźwiękiem. Po przeprowadzeniu postępowania wyjaśniającego w sprawie, Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił uwzględnienia wniosku[117]. Jednakże z uwagi na to, iż w sprawie brak było wystarczających dowodów na to, by spółka poinformowała skarżące o tym, że za pomocą monitoringu będzie rejestrowany również dźwięk, Generalny Inspektor Ochrony Danych Osobowych wystosował do spółki wystąpienie[118], w którym wskazał na konieczność respektowania odpowiednich zasad przez podmioty stosujące nadzór wideo, w szczególności uczulił na konieczność poinformowania o celu i zakresie stosowanego wideonadzoru, tj. czy rejestruje tylko wizję, czy również fonię, oraz miejscach, w których jest on stosowany. Celem ww. wystąpienia było zarówno podniesienie poziomu wiedzy spółki w zakresie zasad stosowania monitoringu, rozwianie wątpliwości osób nim objętych, co do legalności tych działań, a także zapewnienie przejrzystości i transparentności ww. zasad stosowania monitoringu wobec wszystkich pracowników spółki.

[115] Decyzja GIODO z dnia 8 listopada 2013 r. DOLiS/DEC-1174/13/74083,74086,74094.
[116] Pismo GIODO z dnia 8 listopada 2013 r. DOLiS-440-1455/12/AZ/I/74083.
[117] Decyzja GIODO z dnia 28 sierpnia 2013 r. DOLiS/DEC-871/13/54695,54703,54710,54713.
[118] Pismo GIODO z dnia 6 sierpnia 2013 r. DOLiS-440-389/12/AZ/I/49938.

14) Windykacja

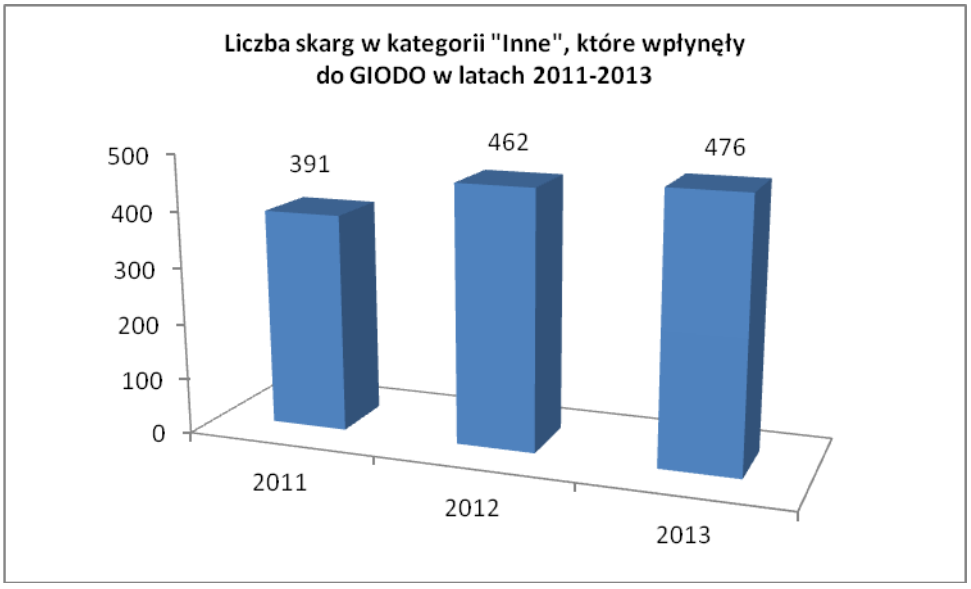
W roku 2013 do organu ds. ochrony danych osobowych wpłynęły **92** skargi dotyczące sektora **windykacji**. Praktycznie wszystkie skargi dotyczyły badania legalności pozyskania i przetwarzania danych osobowych przez firmy windykacyjne.

W jednej ze skarg **na przetwarzanie danych osobowych przez firmę windykacyjną,** skarżąca wskazała, że w jej ocenie fundusz oraz spółka pozyskały i przetwarzają jej dane osobowe niezgodnie z prawem i domagała się ochrony prawnej przewidzianej w ustawie o ochronie danych osobowych. Ponadto skarżąca stwierdziła, że fundusz nabył wierzytelność w drodze umowy cesji wierzytelności z tytułu jej umowy kredytowej, do czego bez zgody skarżącej, w jej ocenie, nie miał prawa. Zdaniem skarżącej fundusz, jako wierzyciel wtórny, pomimo jej żądania nie przedstawił żadnych dokumentów mających świadczyć o zasadności roszczenia, czy prawa do przetwarzania jej danych osobowych. Ponadto skarżąca zwróciła się do tego podmiotu z żądaniem usunięcia jej danych osobowych ze zbiorów danych funduszu, jednakże nie otrzymała odpowiedzi. Skarżąca wówczas wniosła o zbadanie procesu legalności przetwarzania jej danych osobowych przez ww. podmioty oraz o nakazanie przywrócenie stanu zgodnego z prawem, w szczególności poprzez nakazanie usunięcia jej danych osobowych w przypadku stwierdzenia naruszenia przepisów prawa. Generalny Inspektor Ochrony Danych Osobowych dokonał oceny legalności przetwarzania przez fundusz oraz spółkę danych osobowych skarżącej, natomiast nie badał kwestii istnienia lub nieistnienia wierzytelności wobec skarżącej, ani słuszności i zakresu dochodzonych wobec niego roszczeń cywilnoprawnych. W związku z powyższym, po przeprowadzeniu postępowania wyjaśniającego w sprawie, organ w drodze decyzji administracyjnej odmówił uwzględnienia wniosku skarżącej[119].

15) Inne

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2013 r. wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej przedstawionych kategorii spraw. Ich liczba wyniosła **476.**

[119] Decyzja GIODO z dnia 20 grudnia 2013 r. DOLiS/DEC-1338/13/85993,86012,86029.



Wykres 22: ***Zestawienie porównawcze liczby skarg z sektora „Inne", które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2011–2013.***

W tym miejscu przede wszystkim należy wskazać, że w omawianym sektorze występowały – podobnie jak w latach poprzednich - skargi zawierające zarzut przetwarzania danych osobowych przez proboszczów **parafii Kościoła Katolickiego**.

Jednak podkreślenia wymaga, iż w omawianym okresie sprawozdawczym sądy administracyjne zmieniły linię orzeczniczą kwestionując dotychczasowe stanowisko Generalnego Inspektora w analogicznych sprawach. Dotychczas Wojewódzki Sąd Administracyjny w Warszawie przychylał się do stanowiska Generalnego Inspektora Ochrony Danych Osobowych, iż organ nie posiada kompetencji do wydawania merytorycznych decyzji w sprawach dotyczących wystąpienia z Kościoła Katolickiego. Stanowisko to zostało zakwestionowane w wyrokach wydanych przez Naczelny Sąd Administracyjny. NSA bowiem uznał, iż obowiązkiem Generalnego Inspektora było zbadanie, czy osoby składające skargi na odmowę sprostowania ich danych osobowych przez proboszczów parafii, pomimo złożonych przez nich „oświadczeń woli" o wystąpieniu z Kościoła, skutecznie z niego wystąpiły. W pierwszych orzeczeniach, w analogicznych sprawach, NSA uznał, iż powyższa ocena powinna być dokonywana w oparciu o wewnętrzne przepisy Kościoła Katolickiego[120].

[120] Wyrok NSA z dnia 22 marca 2013 r. (I OSK 597/12); wyrok NSA z dnia 27 marca 2013 r. (I OSK 932/12); wyrok NSA z dnia 27 marca 2013 r. (I OSK 1060/12); wyrok NSA z dnia 4 kwietnia 2013 r. (I OSK 897/12).

W związku z tym Generalny Inspektor podjął się badania procedury kościelnej obowiązującej w poszczególnych parafiach, występując do Kurii Diecezjalnych z prośbą o wskazanie przepisów, jakie obowiązują na terenie poszczególnych diecezji, w obrębie których znajdowały się parafie wskazywane w treści skarg apostatów. W kolejnych natomiast orzeczeniach NSA[121] zmienił swoje dotychczasowe stanowisko, wskazując, iż Generalny Inspektor powinien dokonywać oceny ww. oświadczeń już w oparciu o przepisy powszechnie obowiązujące w Państwie Polskim, a nie wewnętrzne regulacje kościelne.

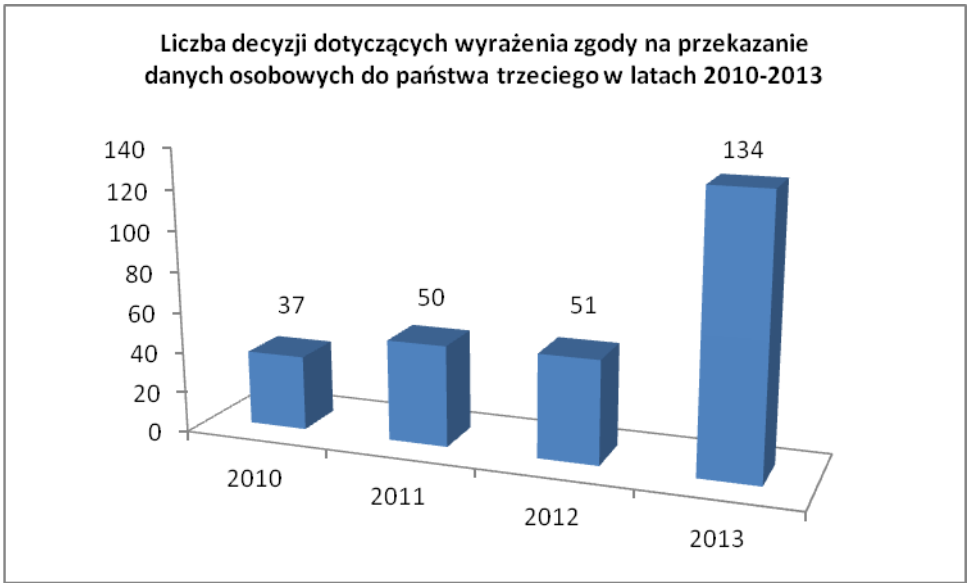
Wobec powyższego Generalny Inspektor musiał podjąć dodatkowe działania mające na celu ustalenie stanowiska organu, które musiało być poprzedzone głęboką analizą orzecznictwa sądów administracyjnych w analogicznych sprawach, a także przepisów prawa dotyczących kwestii wystąpienia z Kościoła Katolickiego, również pod kątem kompetencji Generalnego Inspektora. Na skutek zmiany stanowiska organ do spraw ochrony danych osobowych w drodze decyzji administracyjnych w przedmiotowych sprawach zaczął nakazywać proboszczom parafii rzymskokatolickich przywrócenie stanu zgodnego z prawem poprzez uaktualnienie danych osobowych skarżących, polegające na naniesieniu w księdze chrztów adnotacji o treści zgodnej z żądaniem skarżących[122] lub umarzał postępowanie, jeśli dane zostały sprostowane w toku postępowania toczącego się przed GIODO[123].

3.4. Przekazywanie danych do państw trzecich

Jednym z zadań Generalnego Inspektora Ochrony Danych Osobowych jest rozpatrywanie wniosków o wyrażenie zgody na przekazanie danych do państw trzecich, tzn. do państw nienależących do Europejskiego Obszaru Gospodarczego (EOG) [124]. Zgoda taka jest wymagana, gdy do planowanego transferu danych do państwa trzeciego nie znajdzie zastosowania żadna z przesłanek określonych w art. 47 ustawy.

[121] Wyrok NSA z dnia 18 października 2013 r. (I OSK 1487/12), wyrok NSA z dnia 18 października 2013 r. (I OSK 129/13); wyrok NSA z dnia 24 października 2013 r. (I OSK 1520/13); wyrok NSA z dnia 24 października 2013 r. (I OSK 1828/12).
[122] Decyzja GIODO z dnia 31 grudnia 2013 r. DOLiS/DEC-1358/13/87332,87332.
[123] Decyzja GIODO z dnia 16 października 2013 r. DOLiS/DEC-1101/13/67911,67913.
[124] 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.

W 2013 r. do Generalnego Inspektora wpłynęło **112 wniosków o wyrażenie zgody na przekazanie danych osobowych do państw trzecich,** tj. o 17 więcej w stosunku do 2012 r. W omawianym okresie sprawozdawczym **nastąpił też istotny wzrost wydanych przez Generalnego Inspektora decyzji administracyjnych dotyczących przekazania danych osobowych do państw trzecich, których ogółem było 134.** Niemniej należy zaznaczyć, że część decyzji została wydana w postępowaniach administracyjnych, które zostały zainicjowane w poprzednich latach.



Wykres 23: ***Zestawienie porównawcze liczby decyzji dotyczących wyrażenia zgody na przekazanie danych osobowych do państwa trzeciego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2013.***

Przeważająca większość prowadzonych przez Generalnego Inspektora postępowań administracyjnych została zakończona wydaniem decyzji wyrażającej zgodę na przekazanie danych do państwa trzeciego. W 2013 r., podobnie jak w latach poprzednich, część postępowań wymagała umorzenia w całości bądź w części ze względu na swoją bezprzedmiotowość spowodowaną tym, że państwa, do których miały być przekazane dane osobowe zapewniają odpowiedni poziom ochrony danych osobowych[125], co zostało

[125] Zgodnie z art. 47 ust. 1 ustawy, przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Odpowiedni poziom ochrony danych osobowych, o którym mowa w ust. 1, jest zaś oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel

potwierdzone odpowiednimi decyzjami Komisji Europejskiej wydanymi na mocy art. 25 ust. 6 dyrektywy 95/46/WE[126]. W konsekwencji Generalny Inspektor wydawał decyzje o umorzeniu postępowania w odniesieniu do przekazania danych do odbiorców w Izraelu[127], Nowej Zelandii[128], Urugwaju, Gibraltarze, Baliwatach Guersney i Jersey, czy Argentynie[129]. Również transfer danych do odbiorców w Stanach Zjednoczonych Ameryki, którzy należą do programu „bezpiecznej przystani", nie wymaga uzyskania zgody Generalnego Inspektora[130]. Jednakże ze względu na charakter tego programu należy zaznaczyć, że przekazanie danych w ramach programu może nastąpić jedynie wtedy, gdy certyfikat uczestnictwa w programie obejmuje swoim zakresem kategorie osób, których dane mają być przekazane, kategorie tych danych oraz cele przekazania.

W dotychczasowej praktyce Generalnego Inspektora wątpliwości wzbudzało zastosowanie decyzji 2000/520/WE do dalszego przekazywania danych przez podmiot uczestniczący w programie „bezpiecznej przystani" na zasadzie podpowierzenia podmiotowi spoza programu „bezpiecznej przystani". W poprzednich latach w takich okolicznościach GIODO wymagał zawarcia odpowiednich klauzul lub objęcia transferu wiążącymi regułami korporacyjnymi, a w konsekwencji uzyskania decyzji o wyrażeniu zgody na przekazanie danych. **Jednakże w 2013 r. po analizie Zasad ochrony prywatności w ramach „bezpiecznej przystani" wydanymi przez Departament Handlu USA w dniu 21 lipca 2000 r., które stanowią Załącznik I do decyzji Komisji 2000/520/WE, oraz obecnej praktyki ich stosowania przez władze amerykańskie, GIODO zmienił linię orzeczniczą w tym zakresie**[131]. Oznacza to, że obecnie jeżeli dalsze powierzenie danych przez podmiot uczestniczący w programie „bezpiecznej przystani" odbywa się zgodnie z Zasadami ochrony

---

i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe (ust. 1a).

[126] Aktualna lista decyzji Komisji Europejskiej jest opublikowana na stronie internetowej: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[127] Np. decyzja GIODO nr DESiWM/DEC-61/13/3943; decyzja GIODO nr DESiWM/DEC-128/8390/13.

[128] Decyzja GIODO nr DESiWM/DEC-57/13/3916

[129] Decyzja GIODO nr DESiWM/DEC-902/13/56294, decyzja GIODO nr DESiWM/DEC-903/13/56301.

[130] W dniu 26 lipca 2000 r. Komisja Europejska wydała decyzję 2000/520/WE w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu Stanów Zjednoczonych Ameryki (Dz. Urz. WE 215, 25.8.2000).

[131] np. decyzje GIODO: DESiWM/DEC-160/13/99694, DESiWM/DEC-278/13/15215

prywatności, a w szczególności poprzez zawarcie pisemnej umowy, to nie wymaga się już uzyskania zgody Generalnego Inspektora[132].

Tak jak w latach ubiegłych administratorzy planujący przekazanie danych do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony danych osobowych, najczęściej stosowali standardowe klauzule umowne zatwierdzone przez Komisję Europejską[133]. Należy również odnotować wnioski dotyczące 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 GIODO. 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 GIODO 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

---

[132] Zgodnie z Zasadami ochrony prywatności kwestie dalszego przekazywania danych zostały uregulowane w następujący sposób: w celu ujawnienia informacji stronie trzeciej, organizacje muszą stosować zasady ogłoszenia i wyboru („Notice and Choice Principle). W przypadku gdy organizacja chce przesłać informację stronie trzeciej, będącej przedstawicielem, jak opisano w przypisie końcowym, może to zrobić pod warunkiem uprzedniego upewnienia się, iż strona trzecia przystąpiła do Zasad albo podlega dyrektywie 95/46/WE albo ustaleniom dotyczącym adekwatności lub zawrze z taką stroną trzecią pisemną umowę wymagającą, aby strona trzecia zapewniła, co najmniej taki sam poziom ochrony prywatności, jaki jest wymagany przez odnośne Zasady. Jeżeli organizacja będzie przestrzegać tych wymagań, to nie będzie ona ponosić odpowiedzialności (o ile organizacja nie postanowi inaczej) za to, że strona trzecia, do której przekazuje informacje, przetwarza je w sposób niezgodny z ograniczeniami albo oświadczeniami, chyba że organizacja ta wiedziała albo powinna była wiedzieć, że strona trzecia może przetwarzać dane w taki nieodpowiedni sposób i organizacja nie podjęła właściwych kroków, żeby zapobiec takiemu przetwarzaniu danych lub je powstrzymać. Zgodnie zaś z przypisem końcowym nie jest konieczne uprzedzanie ani oferowanie wyboru, gdy ujawnia się dane stronie trzeciej, która działa jako przedstawiciel powołany do wykonania zadania(-ń) w imieniu i na polecenie organizacji. Z drugiej strony, w takich przypadkach stosuje się zasadę dalszego przekazywania danych.

[133] 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.

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 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 wnioski z załączonymi do nich dokumentami, które nie spełniają wymogów ustawy z dnia 7 października 1999 r. o języku polskim[134]. Generalny Inspektor otrzymał również wniosek, który został złożony w całości w języku angielskim bezpośrednio przez spółkę matkę administratora danych mającego siedzibę na terytorium RP. Jednakże wobec nieusunięcia braków formalnych wniosek ten został pozostawiony bez rozpoznania[135].

[134] Dz. U. 1999 r. Nr 90, poz. 999 z późn. zm.
[135] Sygn. akt DESiWM-41-54/13

W 2013 r. należy odnotować powtarzające się problemy związane z niedopełnieniem przez administratorów danych, planujących transfer danych do państwa trzeciego, obowiązków związanych z przetwarzaniem danych na terytorium RP, które mogą mieć znaczenie dla oceny zgodności z prawem przekazywania danych do państw trzecich. Dotyczyło to zarówno niedopuszczalności przetwarzania w świetle polskiego prawa określonych kategorii danych (np. danych ujawniających pochodzenie etniczne pracowników)[136], czy dużo częściej niespełnienia obowiązku zgłoszenia do rejestracji bądź aktualizacji prowadzonych zbiorów danych osobowych.

Tak jak w poprzednim okresie sprawozdawczym GIODO w 2013 r. stosował kompleksowe podejście do prowadzenia postępowań o wyrażenie zgody na przekazanie danych do państwa trzeciego w sytuacji zastosowania WRK . I tak, biorąc pod uwagę globalny charakter WRK, GIODO 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 GIODO 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[137].

[136] DESiWM/DEC-501/13/26877
[137] Np. DESiWM/DEC-1248/13/82235, DESiWM/DEC-1249/13/82240, DESiWM/DEC-1250/13/82242, DESiWM/DEC-1251/13/82245, DESiWM/DEC-1252/13/82247.

4. Rozpatrywanie zawiadomień o naruszeniu danych osobowych

Jak już była o tym wcześniej mowa, z dniem 22 marca 2013 r. weszły w życie znowelizowane przepisy ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.), które poza zdefiniowaniem pojęcia „naruszenia danych osobowych" wprowadziły m.in. obowiązek zawiadomienia Generalnego Inspektora Ochrony Danych Osobowych przez dostawców publicznie dostępnych usług telekomunikacyjnych, o przypadkach naruszenia danych osobowych abonentów lub użytkowników końcowych będących osobami fizycznymi. Znowelizowane przepisy wprowadziły także obowiązek prowadzenia przez dostawców rejestru naruszeń danych osobowych oraz określiły zakres informacji, jakie powinny się w nim znaleźć. Dostawcy mogą prowadzić rejestr samodzielnie lub powierzyć jego prowadzenie w drodze umowy innemu przedsiębiorcy.

W związku z powyższym, na podstawie § 1 ust. 2 pkt 3, § 2 ust. 1 oraz § 14 ust. 7 Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych, stanowiącego załącznik nr 1 do Zarządzenia nr 1/2012, powołany został Zespół do Spraw Naruszeń Danych Osobowych (Zespół), który bezpośrednio podlega Generalnemu Inspektorowi Ochrony Danych Osobowych. Do zadań Zespołu należy organizacja i koordynacja przyjmowania oraz rozpatrywania zawiadomień o naruszeniu danych osobowych w oparciu o instrukcję postępowania wprowadzoną Zarządzeniem nr 6/2013 Generalnego Inspektora Ochrony Danych Osobowych z dnia 8 marca 2013 r.[138]

Podmiot obowiązany na podstawie art. 174a ustawy Prawo telekomunikacyjne do zawiadomienia GIODO o naruszeniu danych osobowych, wypełnia formularz udostępniony na stronie internetowej www.giodo.gov.pl w zakładce Elektroniczna Skrzynka Podawcza lub na platformie ePUAP (www.epuap.gov.pl) i za ich pośrednictwem przekazuje go do GIODO. W 2013 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **139 zawiadomień o naruszeniu danych osobowych.**

W uzasadnionych przypadkach Zespół opracowywał projekt wystąpienia GIODO do podmiotu obowiązanego na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych. W przypadku jakichkolwiek wątpliwości co do sposobu załatwienia sprawy, Zespół zwracał się z zapytaniem lub wnioskiem do danej jednostki organizacyjnej Biura GIODO o wydanie

[138] Zarządzenie nr 6/2013 Generalnego Inspektora Ochrony Danych Osobowych z dnia 8 marca 2013 r. w sprawie instrukcji postępowania w zakresie zgłaszanych do Generalnego Inspektora Ochrony Danych Osobowych zawiadomień o naruszeniu danych osobowych.

stosownej opinii lub o podjęcie określonych działań w sprawie – na przykład zlecał przeprowadzenie kontroli sprawdzającej u dostawcy. Natomiast w sytuacji, gdy zawiadomienie zawierało braki, Zespół zwracał się do podmiotu obowiązanego o jego uzupełnienie. Dopiero po dokonaniu wszystkich ustaleń w danej sprawie przygotowywano projekt wystąpienia GIODO, bądź sporządzano stosowne wnioski, zalecenia lub wytyczne, przesyłane następnie do podmiotu obowiązanego.

W analizowanym 2013 r. Generalny Inspektor Ochrony Danych Osobowych skierował 1 wystąpienie do podmiotu obowiązanego w związku z naruszeniem ochrony danych osobowych[139].

Ponadto w 2013 roku GIODO przeprowadził kontrole u operatorów telekomunikacyjnych, które objęły **6 podmiotów.** Wszystkie kontrole przeprowadzone w tym obszarze miały charakter częściowy i miały na celu sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych u operatorów publicznej sieci telekomunikacyjnej, dostawców publicznie dostępnych usług telekomunikacyjnych. W grupie tych podmiotów znalazły się 4 podmioty, które złożyły do GIODO zawiadomienia o naruszeniu danych osobowych. W toku czynności kontrolnych ustalono, że zgłoszenia te wiązały się z wyciekiem danych osobowych przetwarzanych przez te cztery podmioty, z jednej wspólnej bazy danych. Dane te zostały upublicznione w sieci Internet w postaci pliku zawierającego 405833 rekordów. Ponadto ustalono, że po uzyskaniu informacji o upublicznieniu danych osobowych, zablokowano funkcjonowanie serwisu internetowego (serwisu elektronicznego biura obsługi klienta dostępnego z sieci Internet), z którego najprawdopodobniej nastąpił wyciek w/w danych.

Ponadto w analizowanym 2013 r. odbyły się 2 spotkania informacyjno – edukacyjne GIODO z przedstawicielami dostawców publicznie dostępnych usług telekomunikacyjnych, podczas których omawiane były zasady współpracy w kontekście sygnalizowanych przez operatorów problemów w odniesieniu do przyjętej procedury zgłaszania naruszeń, a także przekazywano informacje na temat planowanych przez Komisję Europejską kierunków działań w obszarze związanym z telekomunikacją.

Podkreślenia wymaga, że dnia 25 sierpnia 2013 r. weszły w życie nowe przepisy unijne nakładające dodatkowe obowiązki na dostawców publicznie dostępnych usług

[139] Wystąpienie z dnia 27 sierpnia 2013 r. sygn. GI-030-1/13/57913.

telekomunikacyjnych. Zostały one określone w Rozporządzeniu Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej. Rozporządzenie jest wiążące w całości i ma bezpośrednie zastosowane we wszystkich państwach członkowskich. W świetle jego przepisów dostawcy mają obowiązek powiadomienia właściwego organu krajowego o przypadkach naruszenia danych osobowych nie później niż 24 godziny po wykryciu naruszenia (w polskich przepisach termin powiadomienia wynosi 3 dni). Rozporządzenie przewiduje m.in. możliwość wstępnego powiadomienia, jeżeli nie wszystkie informacje są dostępne i konieczne jest dalsze badanie przypadku naruszenia danych osobowych, określa zakres informacji, jakie powinno zawierać takie wstępne powiadomienie oraz przewiduje możliwość aktualizowania wcześniej przekazanych informacji (w polskich przepisach brak jest takich zapisów). Zgodnie z rozporządzeniem powiadomienie skierowane do abonenta lub osoby fizycznej powinno być sformułowane w sposób jasny i łatwo zrozumiały, a dostawca nie może wykorzystywać powiadomienia jako okazji do promowania lub reklamowania nowych lub dodatkowych usług. Jednocześnie przewiduje ono możliwość powiadomienia osób, których dostawca nie jest w stanie zidentyfikować, a wobec których naruszenie prawdopodobnie ma niekorzystne skutki, poprzez ogłoszenia w głównych mediach krajowych lub regionalnych (w polskich przepisach brak jest analogicznych zapisów).

5. Egzekwowanie obowiązków o charakterze niepieniężnym określonych w decyzjach administracyjnych GIODO

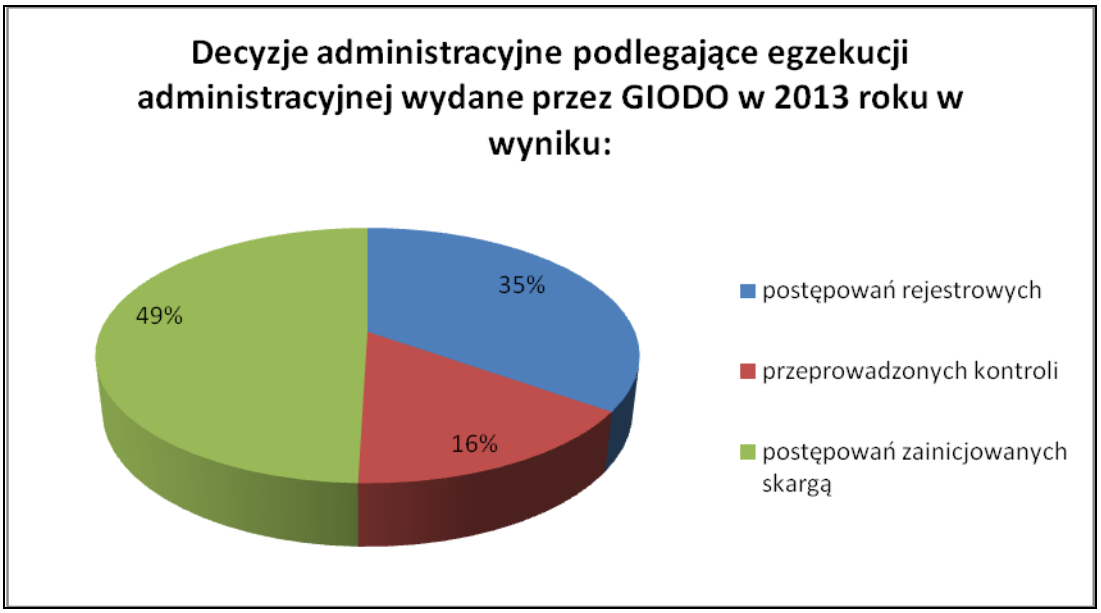
W celu zapewnienia wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych, Generalny Inspektor - na podstawie art. 12 pkt 3 ustawy o ochronie danych osobowych - uprawniony jest do stosowania środków egzekucyjnych przewidzianych w ustawie 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[140], a obowiązki z zakresu ochrony danych osobowych nakładane w drodze wydawanych przez niego decyzji, zostały dodane do katalogu obowiązków podlegających egzekucji administracyjnej[141].

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 zawiera postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlega 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.

W 2013 r. Generalny Inspektor wydał **109 decyzji administracyjnych** zawierających nałożony na strony nakaz (obowiązek) do wykonania i **podlegających egzekucji administracyjnej**. Spośród decyzji wydanych w 2013 r. **38** (35 %) dotyczyło postępowań rejestrowych, **17** (16 %) zostało wydanych w związku z przeprowadzonymi kontrolami, **54** (49 %) wydano na skutek postępowania zainicjowanego skargą.

[140] art. 20 § 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji.
[141] art. 2 § 1 pkt 12 cyt. w. ustawy o postępowaniu egzekucyjnym w administracji.



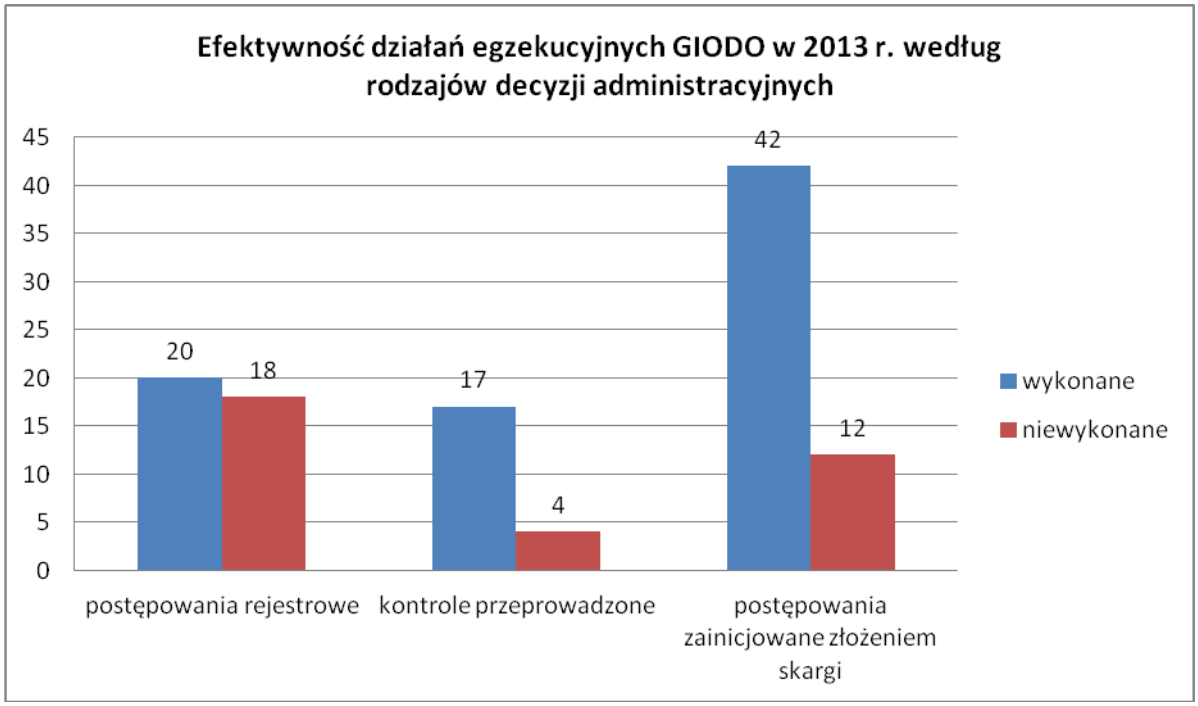
Wykres 24: ***Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji, wydanych przez GIODO w 2013 r.***

Efektywność prowadzonych w 2013 r. przez Generalnego Inspektora działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków, przedstawia się następująco: spośród 109 decyzji administracyjnych **wykonanych zostało przez zobowiązanych 75 decyzji**, 34 decyzji na koniec 2013 r. pozostało niewykonanych. Decyzje te objęte są działaniami egzekucyjnymi w 2014 r. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań Generalnego Inspektora Ochrony Danych Osobowych oraz przeprowadzonych kontroli sprawdzających. W 16 przypadkach wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia zobowiązani w 13 przypadkach wykonali w całości decyzję administracyjną GIODO.

Wobec 3 zobowiązanych wystawiony został tytuł wykonawczy i wszczęte zostało postępowanie egzekucyjne. W 2 przypadkach zastosowany został środek egzekucyjny w postaci nałożenia grzywny w celu przymuszenia (w obu przypadkach wysokość grzywny wyniosła 25.000 zł). Postępowania egzekucyjne nie zostały zakończone w 2013 r. i będą kontynuowane w 2014 r. Nałożone grzywny w celu przymuszenia nie zostały przez zobowiązanych uiszczone dobrowolnie. W związku z powyższym wystawione zostały przez Generalnego Inspektora tytuły wykonawcze i skierowane zostały wnioski o wszczęcie postępowania egzekucyjnego obowiązków o charakterze pieniężnym do właściwych

naczelników urzędów skarbowych. W obu przypadkach postępowanie egzekucyjne zakończyło się powodzeniem, grzywny zostały w drodze egzekucji uiszczone.

Spośród decyzji wydanych w 2013 r. i wykonanych przez zobowiązanych w 2013 r. **20** dotyczyło postępowań rejestrowych, **13** zostało wydanych w związku z przeprowadzonymi kontrolami, **42** wydano na skutek postępowania zainicjowanego skargą. Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w 2013 r. wynosił **69%.** W odniesieniu do postępowań rejestrowych efektywność egzekucji wynosiła **53%**, wobec decyzji wydanych w związku z przeprowadzonymi kontrolami - **76%**, natomiast w stosunku do decyzji wydanych na skutek postępowań zainicjowanych skargą - **78%**.



Wykres 25: ***Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2013 r.***

Wykres 26: ***Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji, wydanych przez GIODO w 2013 r.***

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

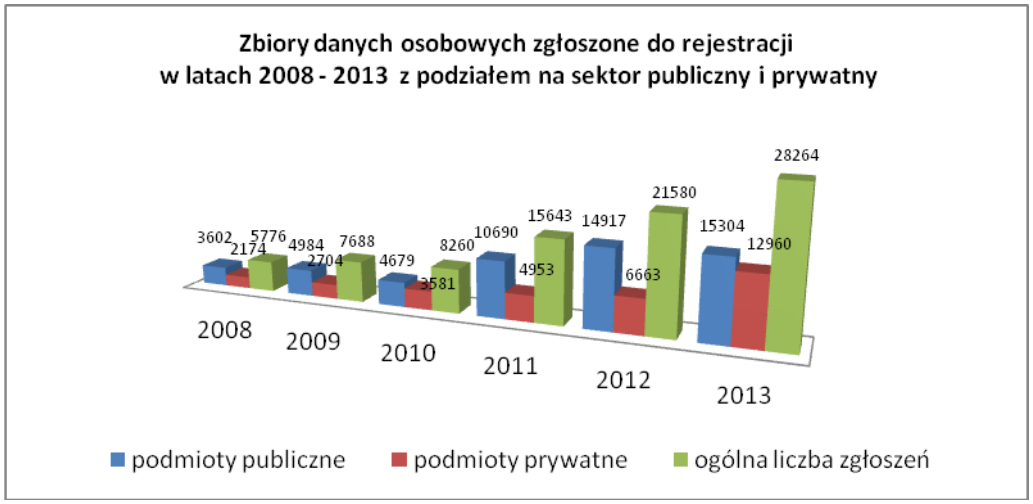
Jednym z podstawowych zadań Generalnego Inspektora Ochrony Danych Osobowych, zgodnie z art. 12 pkt 4 oraz art. 42 ust. 1 ustawy o ochronie danych osobowych, jest prowadzenie ogólnokrajowego, jawnego rejestru zbiorów danych osobowych.

Głównym celem rejestracji zbiorów danych osobowych jest zapewnienie przejrzystości w sferze przetwarzania danych osobowych oraz stworzenie warunków do sprawowania indywidualnej oraz urzędowej kontroli nad przestrzeganiem zasad przyjętych w ustawie o ochronie danych osobowych. Prowadzenie ogólnokrajowego rejestru zbiorów danych osobowych zapewnia bowiem wszystkim zainteresowanym dostęp (w tym również za pośrednictwem platformy internetowej e-GIODO) do informacji o administratorach danych i prowadzonych przez nich zbiorach danych osobowych, a także umożliwia Generalnemu

Inspektorowi Ochrony Danych Osobowych m.in. sprawowanie kontroli nad prawidłowością procesu przetwarzania danych osobowych. W razie stwierdzenia niezgodności przetwarzania danych z przepisami o ochronie danych osobowych, możliwe jest wyeliminowanie zaistniałych uchybień, już na etapie postępowania rejestracyjnego.

Informacje uzyskane w toku postępowania rejestracyjnego stanowią dla Generalnego Inspektora Ochrony Danych Osobowych podstawowe źródło wiedzy na temat administratorów danych, prowadzonych przez nich zbiorów danych oraz warunków przetwarzania danych w tych zbiorach. Posiadanie tych informacji pozwala zdefiniować problemy występujące w procesie przetwarzania danych w określonych obszarach i podjąć działania zmierzające do przywrócenia stanu zgodnego z prawem.

W 2013 roku, administratorzy danych, wypełniając obowiązek określony w art. 40 ustawy o ochronie danych osobowych[142], **zgłosili do rejestracji** Generalnemu Inspektorowi Ochrony Danych Osobowych **28264 zbiory**, z czego podmioty z sektora administracji publicznej zgłosiły 15304 zbiory, co stanowi 54 % ogólnej liczby zgłoszeń dokonanych w tym okresie, a podmioty z sektora prywatnego 12960 zbiorów, co stanowi 46 % ogólniej liczby zgłoszonych zbiorów.

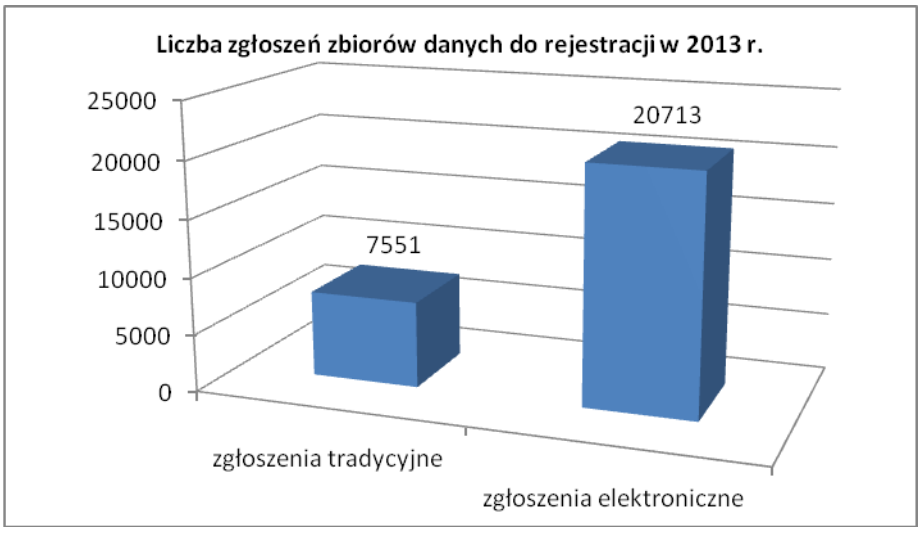


Wykres 27: ***Liczbowe zestawienie zbiorów danych osobowych zgłoszonych do rejestracji przez podmioty publiczne i prywatne w latach 2008 - 2013.***

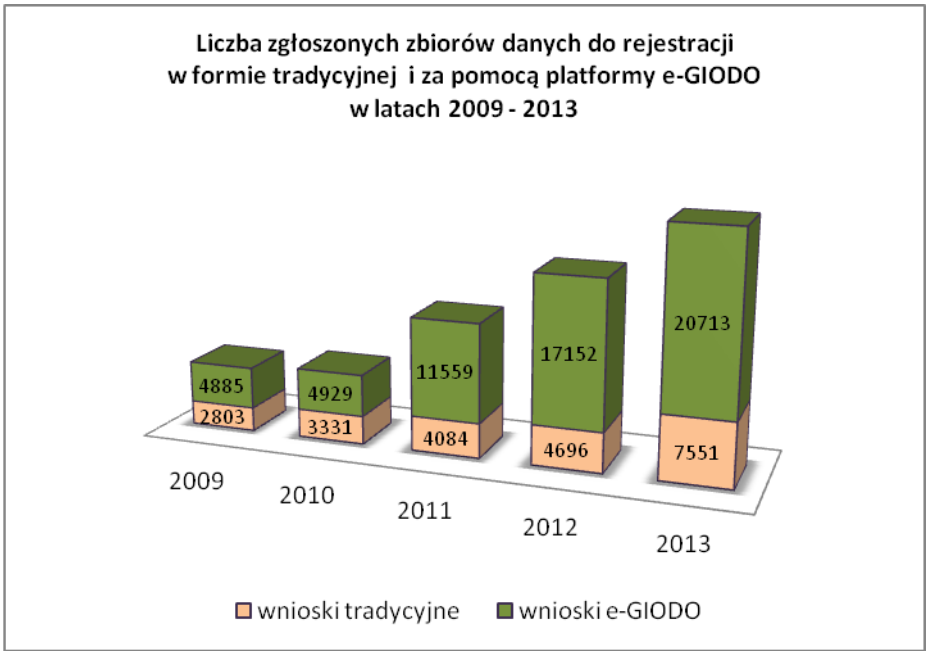
[142] Zgodnie z art. 40 ustawy administrator danych obowiązany jest zgłosić zbiór danych do rejestracji, z wyjątkiem przypadków określonych w art. 43 ust. 1 ustawy.

Analizując powyższy wykres należy zauważyć **wzrost (w stosunku do roku 2012 o 31 %, w stosunku do roku 2011 o 81 %, zaś w stosunku do roku 2010 aż o 242 %) liczby zgłoszeń nadesłanych do rejestracji w 2013 roku.** Ponadto należy wskazać, że coraz więcej zgłoszeń zbiorów pochodzi od podmiotów prywatnych – w 2013 r. nastąpił wzrost liczby zgłoszeń pochodzących od tej grupy podmiotów o 95 % w stosunku do 2012 r., podczas gdy wzrost zgłoszeń składanych przez podmioty publiczne w tym samym okresie wyniósł 3 %. W konsekwencji w roku sprawozdawczym już 46 % ogólnej liczby zgłoszonych zbiorów pochodziło od podmiotów prywatnych, podczas gdy zarówno w roku 2012 jak i 2011 wskaźnik ten wynosił 31 - 32 %.

W roku 2013 roku **przy użyciu programu wspomagającego (eGIODO)**, udostępnionego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych, **zgłoszono do rejestracji 20713 zbiorów danych.** Zgłoszenia dokonane drogą elektroniczną stanowiły 73 % wszystkich zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2013 r. Jest to wynik porównywalny do poprzednich okresów sprawozdawczych (2012 – 78 %, 2011 – 74 %). Program komputerowy służący do realizacji obowiązku rejestracji drogą elektroniczną zawiera system podpowiedzi, co pozwala zwiększyć liczbę zgłoszeń, które zawierają informacje określone w art. 41 ust. 1 ustawy. Program jest modyfikowany, tak aby ograniczyć możliwość popełnienia błędu przy wypełnieniu zgłoszenia.



Wykres 28: ***Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonanych w 2013 r. w formie tradycyjnej i elektronicznej.***



Wykres 29: ***Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2009 - 2013 r. w formie tradycyjnej i przy użyciu elektronicznego programu wspomagającego, udostępnionego na stronie www.giodo.gov.pl***

Liczba **zakończonych postępowań** prowadzonych w związku ze zgłoszeniami zbiorów do rejestracji w okresie sprawozdawczym wyniosła **17884**. Zdecydowana większość prowadzonych postępowań zakończyła się wpisem zbioru danych do rejestru, który dokonywany jest w drodze czynności materialno-technicznej.

W okresie sprawozdawczym do ogólnokrajowego, jawnego rejestru zbiorów danych osobowych prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych **zostało wpisanych 16866 zbiorów danych**, tj. o 599 zbiorów więcej niż w roku 2012 i o 5021 zbiorów więcej niż w roku 2011.

Wykres 30: ***Zestawienie porównawcze zarejestrowanych zbiorów danych osobowych w ogólnokrajowym rejestrze w latach 2008 - 2013.***

Chociaż liczba zarejestrowanych zbiorów danych osobowych stale rośnie, w wielu przypadkach przesłane zgłoszenia nie spełniały wymogów formalnych przewidzianych w ustawie z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r. poz. 267). W konsekwencji w 2013 roku skierowano do wnioskodawców, na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego, **867 wezwań do uzupełnienia w zgłoszeniu braków formalnych**. Wezwania dotyczyły przede wszystkim niespełnienia wymogów w zakresie podpisania zgłoszenia składanego w formie pisemnej lub braku uwierzytelnienia w przypadku wniesienia zgłoszenia w formie dokumentu elektronicznego. W **298 pismach**, w związku z nieuzupełnieniem braku formalnego, poinformowano wnioskodawców o **pozostawieniu zgłoszenia bez rozpoznania**.

Również w wielu przypadkach informacje zawarte w zgłoszeniu nie pozwalały na zakończenie sprawy bez przeprowadzenia postępowania wyjaśniającego. W 2013 roku w toku postępowań rejestracyjnych do wnioskodawców **skierowano 1654 pisma**, w których Generalny Inspektor Ochrony Danych Osobowych **zwracał się o złożenie pisemnych wyjaśnień oraz informował o uprawnieniach strony przed wydaniem decyzji administracyjnej** (wzrost o 19 % w stosunku do roku 2012). Wyjaśnienia w prowadzonych postępowaniach dotyczyły 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 jej trakcie ustala się, czy

zgłoszenie faktycznie dotyczy zbioru danych, czy zbiór został zgłoszony przez podmiot zobowiązany, 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 nie występują przesłanki zwolnienia z obowiązku rejestracji określone w art. 43 ust. 1 ustawy[143].

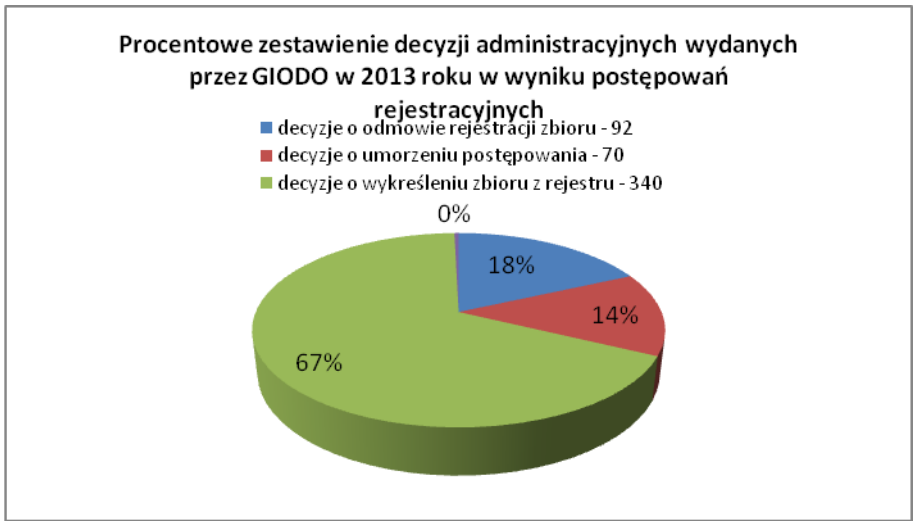
W 2013 roku wysłano do wnioskodawców **505** pism informujących o braku obowiązku rejestracji zbioru, wynikającym z przesłanek określonych w art. 43 ust. 1 ustawy oraz **351** pism informujących o braku podstaw do dokonania wpisów w rejestrze z innych przyczyn, niż wynikające z powołanego powyżej przepisu. Dotyczyły one głównie zgłoszeń dokonanych przez 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.

Jeżeli zgłoszenie pozytywnie przejdzie wstępną weryfikację, to w kolejnym etapie ustala się, czy nie zachodzi przesłanka odmowy rejestracji zgłoszonego zbioru danych. Zgodnie bowiem 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

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

warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy. Zatem w postępowaniu rejestracyjnym ocenie poddawany jest m.in. zakres przetwarzanych danych, tj. czy jest on adekwatny w stosunku do celu w jakim prowadzony jest zbiór. Administrator danych zobowiązany jest bowiem gromadzić tylko te dane, które są niezbędne ze względu na cel ich przetwarzania. Badaniu podlega też legalność przetwarzania danych - w tym celu dokonywana jest m.in. analiza przepisów prawa regulujących zadania lub działalność, w związku z realizacją których administrator przetwarza dane osobowe w zbiorze - oraz wypełnienie warunków technicznych i organizacyjnych, o których mowa 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), tj. zastosowanie środków bezpieczeństwa na odpowiednim poziomie.

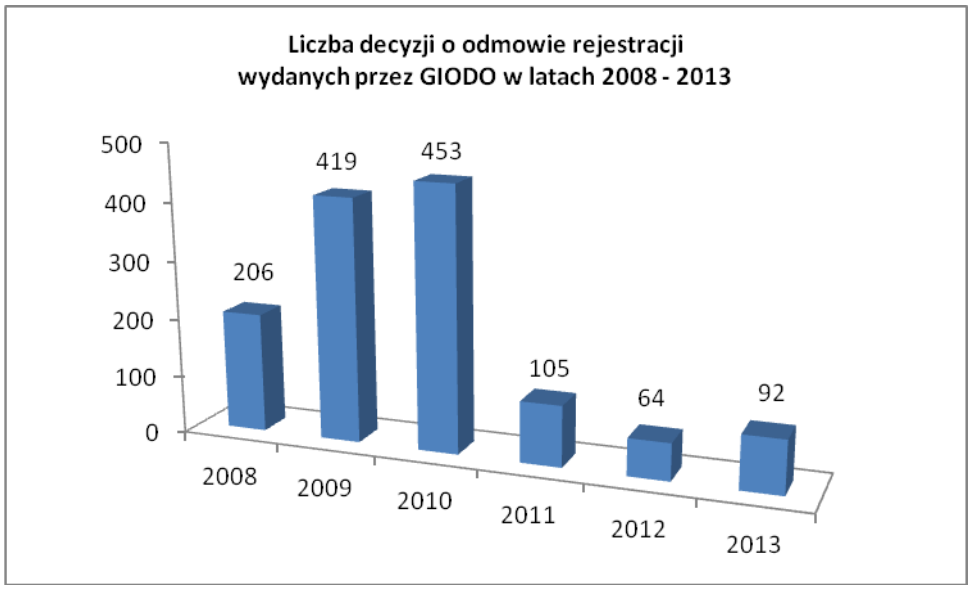
W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał ogółem **504 decyzje administracyjne w związku z postępowaniem rejestracyjnym.** Spośród nich **92 decyzje dotyczyły odmowy rejestracji zbioru danych, 70 - umorzenia postępowania, 340 decyzji dotyczyło wykreślenia** zbioru danych z ogólnokrajowego jawnego rejestru zbiorów danych osobowych, zaś **2 decyzje wydano po ponownym rozpatrzeniu sprawy.**



Wykres 31: ***Procentowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2013 r.***

Wraz z odmową rejestracji zbioru Generalny Inspektor Ochrony Danych Osobowych 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 duży 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.

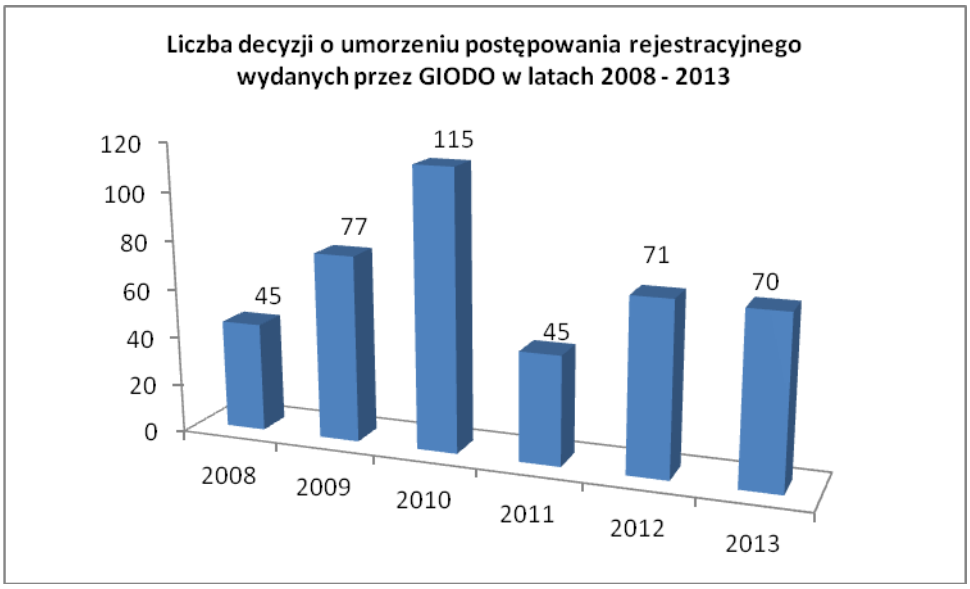
W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **92 decyzje o odmowie rejestracji zbioru danych.**



Wykres 32: ***Zestawienie porównawcze liczby decyzji o odmowie rejestracji zbioru wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 – 2013.***

Ponadto wydanych zostało **70 decyzji o umorzeniu postępowania rejestracyjnego** (najczęściej w sytuacji, gdy w toku postępowania wnioskodawca wycofał zgłoszenie np. informując, że nie rozpoczął przetwarzania danych w zbiorze, zrezygnował z utworzenia zbioru danych osobowych)**, w tym 1 decyzja umarzająca postępowanie w sprawie po jej**

ponownym rozpatrzeniu oraz **2 inne decyzje po ponownym rozpatrzeniu sprawy.**

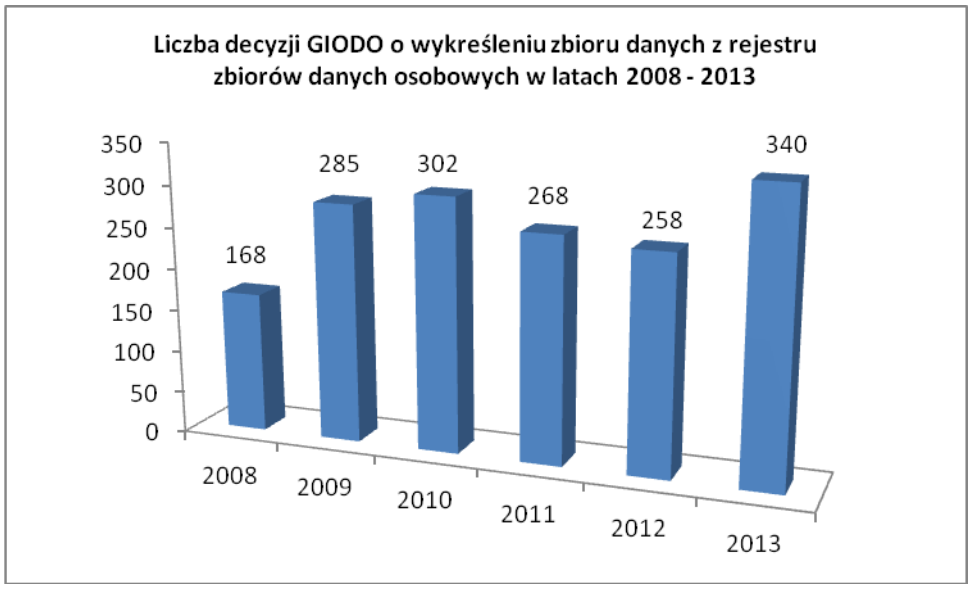


Wykres 32: ***Zestawienie porównawcze liczby decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2013.***

W przypadku wydania decyzji o odmowie rejestracji zbioru administrator danych, zgodnie z art. 44 ust. 4 ustawy o ochronie danych osobowych, może zgłosić ponownie zbiór danych do rejestracji po usunięciu wad, które były powodem odmowy jego rejestracji. Jednocześnie nakazy zawarte w decyzjach o odmowie rejestracji zbioru danych osobowych podlegają egzekucji w trybie określonym w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2012 r. poz. 1015 z późn. zm.). W związku z powyższym, jeżeli administrator nie dokonał ponownego zgłoszenia zbioru do rejestracji lub gdy informacje zawarte w zgłoszeniu wskazywały, że wady, które były powodem wydania decyzji, nie zostały przez administratora usunięte, ostateczne decyzje o odmowie rejestracji zbioru danych przekazywane były do Zespołu do Spraw Egzekucji Administracyjnej. Większość administratorów danych dobrowolnie wykonała nakazy zawarte w decyzji o odmowie rejestracji.

Generalny Inspektor Ochrony Danych Osobowych wydał **340 decyzji o wykreśleniu** zbioru danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych z powodu zaprzestania przetwarzania danych w zbiorze. Należy przy tym zaznaczyć, iż decyzja ta może dotyczyć więcej niż jednego zbioru danych osobowych. Ostateczna decyzja o wykreśleniu

zbioru danych stanowi podstawę do dokonania czynności materialno-technicznej, tj. wykreślenia zbioru z ogólnokrajowego, jawnego rejestru zbiorów danych – **w 2013 roku wykreślono z rejestru 449 zbiorów danych osobowych** (32 % więcej niż w roku 2012).



Wykres 33: ***Zestawienie porównawcze liczby decyzji o wykreśleniu zbioru danych z rejestru, wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2013.***

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 (zgodnie z art. 41 ust. 2 ustawy administrator danych obowiązany jest zgłaszać każdą zmianę informacji zawartych w zgłoszeniu rejestracyjnym w terminie 30 dni od dnia dokonania zmiany w zbiorze danych), a z drugiej strony, instytucja wykreślenia zbioru, dające możliwość porządkowania rejestru, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych.

W 2013 roku **rozpatrzonych zostało 3709 zgłoszeń aktualizacyjnych** dokonanych przez administratorów danych na podstawie art. 42 ust. 2 ustawy.

Wykres 34: ***Zestawienie porównawcze liczby zgłoszeń aktualizacyjnych rozpatrzonych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2013.***

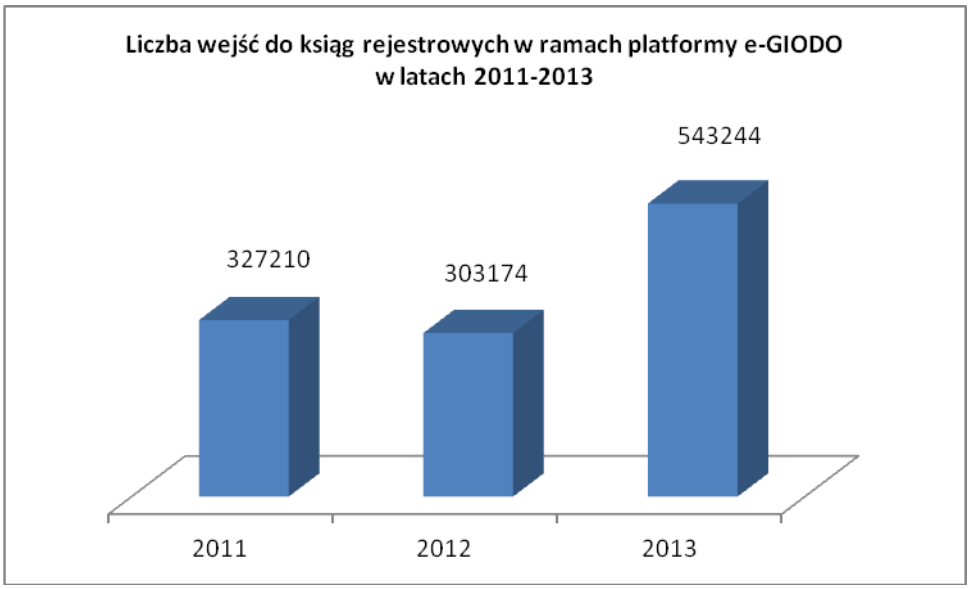
Ponadto Generalny Inspektor Ochrony Danych Osobowych wydał w omawianym okresie **2863 zaświadczenia o zarejestrowaniu zbioru danych.** W przypadku zarejestrowania zbioru danych, w którym przetwarzane są dane osobowe szczególnie chronione, określone w art. 27 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wydaje zaświadczenie z urzędu, niezwłocznie po dokonaniu rejestracji takiego zbioru[144]. Administrator danych może także wystąpić z wnioskiem do Generalnego Inspektora Ochrony Danych Osobowych o wydanie zaświadczenia o zarejestrowaniu zbioru[145].

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) w ramach elektronicznej platformy e-GIODO. Wyszukanie ksiąg rejestrowych dotyczących zbiorów wpisanych do ogólnokrajowego rejestru

[144] Art. 42 ust. 4 ustawy
[145] Art. 42 ust. 3 ustawy

zbiorów danych osobowych możliwe jest według różnych kryteriów, m.in. nazwy administratora danych, miejscowości, czy też nazwy zbioru danych.

W roku 2013 w elektronicznej wersji rejestru odnotowano **543244 wejść** do poszczególnych ksiąg rejestrowych, tj. o 240069 więcej w stosunku do poprzedniego roku sprawozdawczego, w którym zarejestrowano 303175 takich wejść.



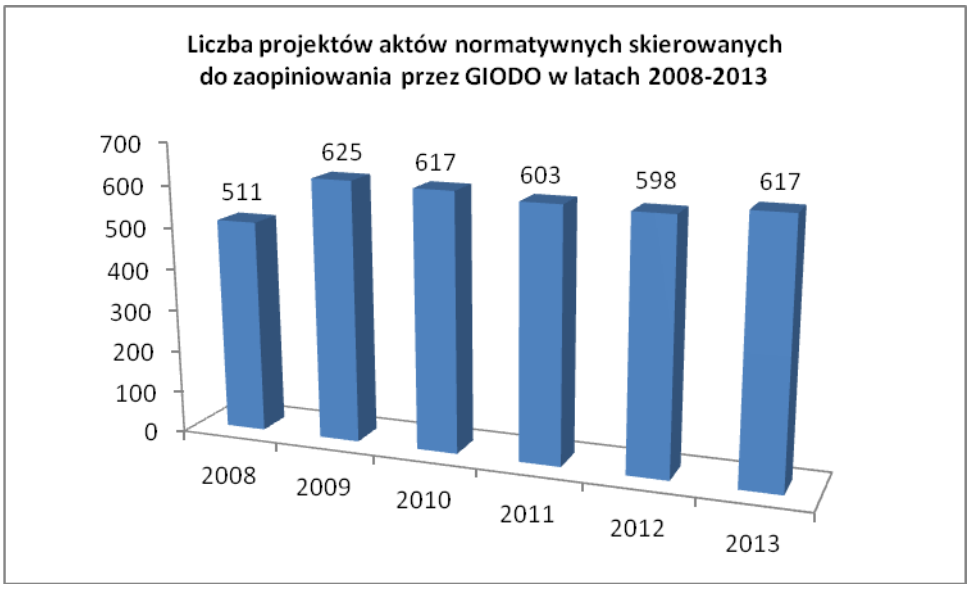
Wykres 35: ***Liczbowe zestawienie wejść do poszczególnych ksiąg rejestrowych w rejestrze zbiorów danych osobowych w ramach platformy e-GIODO w latach 2011 - 2013.***

Mając na uwadze wzrost świadomości obywateli w zakresie przysługujących im uprawnień w związku z przetwarzaniem dotyczących ich danych osobowych podkreślić należy, że jawny rejestr zbiorów danych osobowych stanowi istotne narzędzie pozwalające im efektywnie z tego prawa korzystać. Rozwój świadomości prawnej administratorów danych w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych, w tym obowiązku **rejestracji zbiorów danych osobowych**, przyczynił się do zauważalnego wzrostu liczby zgłoszeń zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

7. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych

Eliminowaniu nieprawidłowości dotyczących przetwarzania danych osobowych już na etapie 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 2013 do Biura GIODO wpłynęło do zaopiniowania **617 projektów aktów prawnych,** tj. o 19 więcej w stosunku do roku 2012, w którym wpłynęło 598 projektów.



Wykres 36: ***Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2013.***

W podziale na poszczególne miesiące 2013 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła następująca liczba projektów aktów prawnych: styczeń - 53, luty - 58, marzec - 43, kwiecień - 46, maj - 50, czerwiec - 53, lipiec - 54, sierpień - 52, wrzesień - 48, październik - 66, listopad - 57, grudzień - 37. **W sumie 617.**

W okresie sprawozdawczym Generalnemu Inspektorowi przedstawiono do zaopiniowania dokument pt. „**Projekt założeń projektu ustawy o prawach pacjenta**

i Rzeczniku Praw Pacjenta”[146], wobec którego wyraził pełną aprobatę dla przyjętego w nim kierunku zmian w zakresie zasad związanych z postępowaniem z dokumentacją medyczną. Dotychczasowy bowiem brak precyzyjnego określenia w przepisach tychże zasad oraz wątpliwości dotyczące przetwarzania danych osobowych w związku z postępowaniem prowadzonym przed wojewódzkimi komisjami do spraw orzekania o zdarzeniach medycznych – sygnalizowane już wcześniej przez GIODO – negatywnie wpływały na możliwość zapewnienia przez administratorów danych właściwego poziomu ochrony danych osobowych, w tym tych szczególnie chronionych (art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.).

Generalny Inspektor Ochrony Danych Osobowych przedstawiając uwagi szczegółowe do projektu, wskazał na następujące zagadnienia.

Po pierwsze, zasugerował rozważenie zasadności koncepcji polegającej na nałożeniu na podmioty zobowiązane do przechowywania dokumentacji medycznej, w przypadku zakończenia działalności leczniczej[147], obowiązku wydania tej dokumentacji pacjentom, jako „pierwszego z etapów” postępowania z przedmiotową dokumentacją w tego typu okolicznościach. Generalny Inspektor zgodził się, iż pacjent winien mieć w pierwszej kolejności dostęp do danych zawartych w dokumentacji medycznej[148]. Jednakże trudno było uznać, iż jest on jej jedynym dysponentem, czy właścicielem. Organ do spraw ochrony danych osobowych powołał normę zawartą w art. art. 24 ust. 1 aktualnie obowiązującej ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w którym stwierdza się, że „w celu realizacji prawa, o którym mowa w art. 23 ust. 1, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w niniejszym rozdziale oraz zapewnić ochronę danych zawartych w tej dokumentacji”. GIODO stwierdził ponadto, że ustawodawca wprowadził w tym przepisie pewien obowiązek i nałożył go na określony podmiot, zakładając, iż będzie on dysponował odpowiednią wiedzą, niezbędną, aby właściwie wypełniać swoje obowiązki w zakresie przetwarzania danych zawartych w dokumentacji medycznej. Wobec tego przerzucanie przedmiotowego obowiązku na pacjentów nie może być uznane za rozwiązanie właściwe z punktu widzenia konieczności zapewnienia odpowiedniej ochrony danych

[146] DOLiS-033-496/13
[147] Część III.1.1.1 projektu
[148] Zgodnie z art. 23 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2012 r. poz. 159 z późn. zm.).

znajdujących się w dokumentacji medycznej. Nie można bowiem od takich osób – z jednej strony – wymagać posiadania fachowej wiedzy co do pożądanych sposobów zabezpieczenia danych, z drugiej – żądać zastosowania właściwych warunków techniczno – organizacyjnych (sprzętowo – lokalowych) zapewniających taką ochronę. GIODO stwierdził, że zasadne wydaje się takie ukształtowanie przepisów stanowiących o losie dokumentacji medycznej po zaprzestaniu prowadzenia działalności leczniczej, aby wyeliminować nadmierną uznaniowość w tym zakresie podmiotów tworzących albo sprawujących nadzór nad podmiotem leczniczym lub podmiotów prowadzących właściwe rejestry. Krąg zobowiązanych do przejęcia tego typu dokumentacji winien zostać precyzyjnie wskazany, inaczej, aniżeli wynika to z aktualnie obowiązujących przepisów[149].

Po drugie, odnosząc się do wprowadzenia tzw. instytucji powierzenia przechowywania dokumentacji medycznej przez podmiot udzielający świadczeń zdrowotnych, cyt.: „wzorowanej na rozwiązaniach przewidzianych w (…) ustawie o ochronie danych osobowych (…)”[150], Generalny Inspektor wskazał, iż kwestia braku w aktualnie obowiązujących przepisach podstawy prawnej do przekazywania danych objętych tajemnicą medyczną podmiotom spoza katalogu określonego w art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (w celu korzystania ze specjalistycznych usług w modelu tzw. outsourcingu) była również przedmiotem sygnalizacji ze strony organu do spraw ochrony danych osobowych[151]. Generalny Inspektor Ochrony Danych Osobowych podkreślił, iż administrator danych musi wykazać szczególną ostrożność w doborze odpowiedniego podmiotu, który będzie w jego imieniu i na jego rzecz wykonywał określone czynności związane z przetwarzaniem danych osobowych – w omawianym przypadku – „medycznych danych” pacjentów, a scedowanie na „podmiot zewnętrzny” przez administratora danych swych obowiązków związanych z przechowywaniem dokumentacji medycznej nie może w żaden sposób zwalniać administratora danych z odpowiedzialności za zgodne z prawem

[149]Artykuł 106 ust. 3 pkt 10a oraz art. 106 ust. 4 pkt 8a ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2013 r. poz. 217) stanowią, że do rejestru podmiotów leczniczych – w przypadku podmiotu leczniczego wpisuje się m.in. miejsce przechowywania dokumentacji medycznej w przypadku likwidacji podmiotu leczniczego, a w przypadku praktyki zawodowej – miejsce przechowywania dokumentacji medycznej w przypadku zakończenia działalności leczniczej przez lekarza lub pielęgniarkę – jednak w obu tych przypadkach brak jest jakiegokolwiek zawężenia, czy uściślenia miejsc, w których przechowywanie tego szczególnego rodzaju dokumentacji może się odbywać).

[150] Część III.1.1.3. projektu

[151] Pismo GIODO z dnia 23 sierpnia 2011 r. o sygn. DOLiS-035-2464/11/MM.

przetwarzanie danych przez ten podmiot (art. 31 ust. 4 ustawy o ochronie danych osobowych).

Wątpliwości GIODO wzbudziła także koncepcja prowadzenia dokumentacji medycznej przez osoby, które udzielają świadczeń zdrowotnych, ale nie wykonują działalności leczniczej w rozumieniu ustawy o działalności leczniczej. Wzgląd na specyfikę warunków, w jakich odbywa się udzielanie świadczeń zdrowotnych przez ratowników medycznych działających w ratownictwie górskim, wodnym, narciarskim czy biorących udział w zabezpieczeniu medycznym imprez masowych, przemawia za pogłębioną analizą możliwości zapewnienia właściwych warunków przechowywania tej dokumentacji oraz jej udostępniania. Powstaje jednocześnie pytanie, czy dokumentacja tego typu miałaby stanowić część „ogólnej" dokumentacji medycznej danego podmiotu leczniczego (lub podmiotu innego, niż medyczny). Jeżeli tak, to zaznaczyć należy, iż ta grupa osób nie ma – w aktualnie obowiązującym stanie prawnym – dostępu do dokumentacji medycznej, o której mowa w art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Należy także zastanowić się nad ewentualnymi podstawami prawnymi wymiany dokumentacji pomiędzy podmiotami biorącymi udział w udzielaniu świadczeń zdrowotnych (relacja pomiędzy dokumentacją prowadzoną przez ratowników medycznych oraz podmioty lecznicze).

GIODO wyraził aprobatę wobec zmian legislacyjnych w zakresie statusu komisji do spraw orzekania o zdarzeniach medycznych[152] w odniesieniu do przetwarzania danych osobowych oraz uprawnień przysługujących w tym zakresie wojewodom[153]. Zwrócił jednak uwagę, że z punktu widzenia ochrony danych osobowych doprecyzowania wymaga – w miarę możliwości – zakres informacji, do których będzie miał dostęp wojewoda w związku z orzekaniem przez wojewódzkie komisje do spraw orzekania o zdarzeniach medycznych. Z uwagi na brak kompetencji do dostępu do danych o tak szczególnym charakterze, przewidywany zakres informacji, o których mowa, winien być ograniczony do niezbędnego minimum. Znaczenie odgrywa tu także kwestia wprowadzenia odpowiednich zasad przetwarzania danych osobowych przez ten organ, do których będzie on miał dostęp z uwagi na rozwiązania natury organizacyjnej wynikającej ze specyfiki pracy komisji przyjętej w treści samej ustawy.

[152] Część III.2.2.4 projektu.
[153] Zgodnie z art. 67e ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, siedzibą komisji jest siedziba właściwego urzędu wojewódzkiego).

Natomiast odnosząc się do zmian w zakresie uprawnień Rzecznika Praw Pacjenta[154] Generalny Inspektor wskazał, że konieczna jest analiza wpływu projektowanych zmian na uprawnienia innych organów. Ustalenia wymaga, czy literalne wymienienie Rzecznika Praw Pacjenta wśród „podmiotów uprawnionych", o których stanowi art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, nie pogłębi wątpliwości co do uprawnień w tym zakresie innych organów o podobnym charakterze (np. Rzecznika Praw Dziecka).

Generalny Inspektor zwrócił ponadto uwagę na relację art. 26 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta do art. 444 i n. ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. Nr 16, poz. 93), stanowiących o możliwości dochodzenia m.in. odszkodowania w przypadkach wskazanych w treści przepisów, podnosząc wątpliwość czy ograniczenie prawa wglądu w dokumentację medyczną po śmierci pacjenta wyłącznie do osób upoważnionych przez tegoż pacjenta za życia, nie wpływa negatywnie na możliwość dochodzenia przez osoby uprawnione swoich roszczeń, wynikających z przepisów wskazanego kodeksu.

Odnosząc się do dokumentu pt. **„Projekt założeń projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw"[155],** GIODO zwrócił uwagę na kwestie zarówno objęte nowelizacją, jak i aktualnie obowiązującego stanu, który w jego opinii wymaga zmian.

Nie kwestionując zasadności istnienia rejestrów, które służą ratowaniu zdrowia i życia jednostek, GIODO opowiadał się za prawidłowym uregulowaniem podstawy prawnej ich funkcjonowania. W pierwszej kolejności podniósł, że kwestia przyznania organowi władzy wykonawczej uprawnienia do tworzenia i prowadzenia lub tworzenia i zlecania prowadzenia – w drodze aktu prawnego rangi rozporządzenia – rejestrów medycznych, stanowiących zbiory informacji szczególnie chronionych, których przetwarzanie jest co do zasady zabronione – art. 8 ust. 1 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.1995.281.31 z późn. zm.) oraz art. 27 ust. 1 ustawy o ochronie danych osobowych - pozostaje w jawnej sprzeczności z art. 51 ust. 1 i 5 Konstytucji Rzeczypospolitej Polskiej. Zarówno w świetle standardów

[154] Część III.3. projektu
[155] DOLiS-033-465/13

konstytucyjnych, jak i brzmienia art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, rozporządzenie jest aktem prawnym zbyt niskiej rangi, aby w tak istotny sposób wpływać na prawa i wolności jednostki. Podkreślono w opinii GIODO, że prawo do ochrony prywatności i danych osobowych są prawami osobistymi gwarantowanymi przez Konstytucję RP (art. 47 i art. 51), a co za tym idzie, ograniczenie w zakresie korzystania z przedmiotowych praw (przymusowe umieszczeniu szeregu informacji dotyczących osoby fizycznej w rejestrach prowadzonych przez naczelny organ administracji publicznej lub na jego zlecenie) – wymaga bezdyskusyjnie ustawowej regulacji (art. 31 ust. 3 Konstytucji RP). Stwierdzając powyższe przywołane zostały tezy zawarte w uzasadnieniu orzeczenia Trybunału Konstytucyjnego *„(...) 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. Zasadniczo 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. W takim wypadku zakres materii pozostawionych do unormowania w rozporządzeniu musi być węższy niż zakres materii ogólnie dozwolony na tle art. 92 ust. 1 Konstytucji Rzeczypospolitej Polskiej. Artykuł 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej silniej bowiem akcentuje konieczność szerszego unormowania rangi ustawowej i zawęża pole regulacyjne pozostające dla rozporządzenia (...)*”[156].

Wadliwości tej nie konwaliduje przy tym projektowany przepis art. 19 ust. 4 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 z późn. zm.), który statuuje prawo osoby, której dane dotyczą, do wniesienia sprzeciwu wobec przetwarzania jej danych w rejestrach utworzonych na podstawie kwestionowanych przepisów. W praktyce prawo to – z jednej strony – ma bowiem charakter iluzoryczny – wobec braku obowiązku poinformowania osoby, której dane są przetwarzane, o fakcie zamieszczenia jej danych w którymś z utworzonych rejestrów. Z drugiej zaś – co słusznie zauważył Rzecznik Praw Obywatelskich w treści wniosku skierowanego do Trybunału

[156] Postanowienie z dnia 31 stycznia 2007 r. o sygn. S. 1/2007.

Konstytucyjnego w dniu 19 lipca 2013 r. (sygn. RPO-667915-I/12/KMŁ) o stwierdzenie niezgodności art. 20 ust. 1 w zw. z art. 19 ust. 1 ustawy o systemie informacji w ochronie zdrowia z Konstytucją RP – podaje w wątpliwość niezbędność istnienia rejestrów, skoro ustawodawca przewidział możliwość przeciwstawienia się przez podmiot danych tego rodzaju przetwarzaniu.

GIODO zauważył, że choć projekt przewiduje posługiwanie się przez pracowników medycznych tzw. Kartą Specjalisty Medycznego (KSM), służącą m.in. uwierzytelnieniu posiadacza karty umożliwiając mu dostęp do danych zawartych w rejestrach funkcjonujących w ochronie zdrowia oraz Kartą Ubezpieczenia Społecznego (KUS) w przypadku świadczeniobiorców, to należy jednak rozważyć, czy w aktualnym stanie prawnym konieczne jest posługiwania się przez pacjentów oraz pracowników medycznych numerem PESEL, jako identyfikatorem służącym do dostępu do Systemu Informacji Medycznej (SIM). Wykorzystanie administracyjnego numeru identyfikacyjnego jako identyfikatora w systemach zawierających informacje z zakresu ochrony zdrowia, nie jest rozwiązaniem powszechnie praktykowanym w państwach europejskich, a w niektórych jest nawet wprost zabronione[157]. Ponadto wykorzystywanie numeru PESEL w charakterze loginu osoby korzystającej z systemu informatycznego uznać należy za wysoce kontrowersyjne z punktu widzenia podstawowych zasad bezpieczeństwa tego systemu. Skoro bowiem login jest narzędziem mającym utrudnić osobie nieuprawnionej uzyskanie dostępu do sytemu informatycznego, winien być informacją znaną tylko osobie uprawnionej, która mając ku temu stosowną podstawę, chce z niego skorzystać. Wykorzystanie zatem w charakterze loginu informacji, której pozyskanie nie stanowi w chwili obecnej szczególnego problemu (numery PESEL znajdują się choćby w KRS, mają je też pracodawcy w odniesieniu do wszystkich swoich pracowników), stwarza bezpośrednie niebezpieczeństwo dla danych zgromadzonych w SIM.

Przy okazji rozważań na temat Karty Specjalisty Medycznego Generalny Inspektor zwrócił uwagę na konieczność odpowiedniego przydzielenia uprawnień dostępowych w zależności od wykonywanych w danym podmiocie funkcji. Zgodnie bowiem z treścią zawartą w pkt. 3.5.2. projektu, karty wydawane będą nie tylko osobom wykonującym zawody

[157] Na przedmiotową kwestię GIODO zwracał uwagę przy okazji opiniowania projektu rozporządzenia Ministra Zdrowia regulującego te kwestie. Zob. rozporządzenie Ministra Zdrowia z dnia 11 kwietnia 2013 r. w sprawie sposobu identyfikacji usługobiorców, pracowników medycznych i usługodawców oraz sposobu i trybu przekazywania przez usługodawców informacji o pracownikach medycznych udzielających świadczeń opieki zdrowotnej (Dz. U. z 2013 r. poz. 502).

medyczne, ale i personelowi technicznemu oraz osobom składającym w imieniu świadczeniodawcy oświadczenia woli w relacjach z Narodowym Funduszem Zdrowia. Niedopuszczalnym zatem z punktu widzenia przepisów dotyczących ochrony danych osobowych, ale i np. tajemnic prawnie chronionych, byłoby umożliwienie dostępu do systemu w takim samym zakresie wszystkim osobom posiadającym KSM.

W ramach uwag szczegółowych Generalny Inspektor podniósł kwestię zasadności przetwarzania w bazach danych tego systemu, informacji o wykształceniu oraz stanie cywilnym. Uznał, że zamieszczanie w systemie danych dotyczących wykształcenia personelu medycznego w pewnych sytuacjach znajduje uzasadnienie, jednak pozyskiwanie takiej informacji od innych grup osób, w tym zwłaszcza pacjentów, budzi już zastrzeżenia z uwagi na wątpliwą potrzebę i tym samym pozostawanie takiego uprawnienia w sprzeczności zarówno z cytowanymi wyżej wymogami konstytucyjnymi (art. 51 Konstytucji RP w stosunku do przetwarzania danych przez organy władzy publicznej), jak i z zasadą adekwatności danych w stosunku do celów ich przetwarzania (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych oraz art. 6 ust. 1 lit. c dyrektywy nr 95/46/WE). Z punktu widzenia zasad ochrony danych osobowych nie znajduje żadnego uzasadnienia zamieszczanie w bazach systemu informacji w ochronie zdrowia, danych o stanie cywilnym. Skoro z art. 4 ust. 4 ustawy wynika, iż ww. dane są przetwarzane „wyłącznie w celach statystycznych", to powstaje pytanie o podstawę funkcjonowania systemu w takich celach. Art. 1 ust. 1 ustawy o systemie informacji w ochronie zdrowia, który stanowi o celach funkcjonowania przedmiotowego systemu, w żaden sposób do statystyki się nie odnosi. W związku z szerokim zakresem danych osobowych w nim zamieszczanych, wyłącznie „statystyczne" przetwarzanie informacji dotyczących wykształcenia oraz stanu cywilnego, było – jak się wydaje – dość iluzoryczne.

GIODO ustosunkował się ponadto do koncepcji dodania do rejestru informacji o adresie zameldowania oraz umożliwieniu „przetwarzania (gromadzenia) danych pochodzących z rejestru PESEL" w Centralnym Wykazie Usługobiorców[158].

Odnosząc się do kwestii przetwarzania w rejestrze danych o adresie zameldowania – wobec brzmienia art. 74 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U.

[158] Część 1.6. projektu założeń, zatytułowana „Pozostałe regulacje" w związku z częścią 3.6.2 odnoszącą się do katalogu danych dotyczących usługobiorców.

Nr 217, poz. 1427 z późn. zm.), mającej wejść w życie w dniu 1 stycznia 2015 r. (z wyjątkiem przepisu art. 62) – zgodnie z którym od dnia 1 stycznia 2016 r. znosi się obowiązek meldunkowy – Generalny Inspektor w wątpliwość poddał celowość pozyskiwania przedmiotowej informacji na potrzeby funkcjonowania bazy danych o usługobiorcach działającej w ramach systemu informacji w ochronie zdrowia.

Jeżeli chodzi o rozszerzenie zakresu danych zawartych w Centralnym Wykazie Ubezpieczonych tak, aby ich zakres obejmował wszystkie dane zawarte w zbiorze danych osobowych PESEL (funkcjonującym w oparciu o przepisy ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych – t.j. Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.), a wydaje się, że taki zamiar chciał wyrazić projektodawca, Generalny Inspektor zakwestionował dopuszczalność wprowadzenia do polskiego porządku prawnego tego typu rozwiązania. Powielanie danych funkcjonujących w rejestrze o charakterze ewidencyjnym i przetwarzanie ich na potrzeby rejestrów związanych z systemem informacji w ochronie zdrowia nie może być uzasadnione jedynie „koniecznością zapewnienia niezakłóconego funkcjonowania systemu informacji i dostępu do danych z rejestru PESEL". Generalny Inspektor wskazał, że zakres danych przetwarzanych w rejestrze PESEL obejmuje m.in. nazwiska i imiona poprzednie, imiona i nazwiska rodowe rodziców, imię i nazwisko rodowe małżonka oraz jego nr PESEL, informacje o zawarciu związku małżeńskiego, w tym także dotyczące rozwiązania małżeństwa[159]. Tego typu informacje nie powinny być przedmiotem przetwarzania w ramach systemu informacji w ochronie zdrowia, ponieważ trudno uznać je za dane „niezbędne do prowadzenia polityki zdrowotnej państwa, podnoszenia jakości i dostępności świadczeń opieki zdrowotnej oraz finansowania zadań z zakresu ochrony zdrowia" (art. 1 ust 1 ustawy o systemie informacji w ochronie zdrowia).

GIODO zauważył również, że intencją projektodawcy jest stopniowe poszerzanie uprawnień jednostki podległej Ministrowi Zdrowia (m.in. część 3.6.10. oraz 3.6.16 projektu). Postuluje się tu m.in. wprowadzenie obowiązku dla jednostek organizacyjnych podległych wojewodzie i realizujących zadania z zakresu odbywania specjalizacji, do przekazywania administratorowi systemu informacji w ochronie zdrowia danych o farmaceutach, diagnostach laboratoryjnych i osobach odbywających specjalizację w dziedzinach mających zastosowanie w ochronie zdrowia oraz udostępnianie przez tę jednostkę podmiotom zainteresowanym,

[159] Art. 44a ustawy o ewidencji ludności i dowodach osobistych.

danych z rejestru podmiotów prowadzących działalność leczniczą. Organ do spraw ochrony danych osobowych stoi zaś na stanowisku, iż podmiot, którego ustawowym zadaniem jest pozostawanie „odpowiedzialnym za techniczno – organizacyjną obsługę systemu teleinformatycznego" winien posiadać wyłącznie takie kompetencje, które pozwalają mu na wykonywanie zadań o charakterze „techniczno – organizacyjnym". Rozwiązanie, zgodnie z którym wszelkiego rodzaju uprawnienia, które w pewien sposób sytuują ten podmiot w porządku prawnym na równi z administratorem danych osobowych w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, pozostaje w sprzeczności z przepisami o ochronie danych osobowych. Skoro „jednostka podległa" działa jako „administrator systemu" (a nie jako podmiot, o którym mowa w art. 31 ustawy o ochronie danych osobowych), to wyposażanie jej w kompetencje decyzyjne burzyć może porządek prawny, choćby w zakresie właściwego przypisania odpowiedzialności za ewentualne naruszenie przepisów o ochronie danych osobowych. Jednocześnie powyższe pozostaje w sprzeczności z zasadą wywodzenia odpowiedniego zakresu uprawnień z przepisów kompetencyjnych danego podmiotu.

Organ do spraw ochrony danych osobowych wskazał ponadto na potrzebę doprecyzowania zakresu danych, który w odpowiednim przypadku miałby być przetwarzany. Tytułem przykładu powołał użyte w projekcie lapidarne określenie, iż zapotrzebowanie na lek, wyrób medyczny lub środek spożywczy specjalnego przeznaczenia żywieniowego zawierać będzie m.in. „adres" (bez dookreślenia, o jakiego rodzaju adres chodzi). Wyrażenie to może powodować wątpliwości interpretacyjne, choćby w przypadku lekarzy prowadzących indywidualną praktykę lekarską (część 3.1 projektu). Problem – podnoszony już przez samorząd lekarski – może bowiem dotyczyć konieczności posługiwania się przez takiego lekarza swym prywatnym adresem zamieszkania. Uwzględniając natomiast, iż wykonując swój zawód osoby te winny mieć możliwość udostępniania jedynie tych informacji, które z wykonywaniem zawodu są związane, stworzenie przepisów prawa zapewniających odpowiednią ochronę sferze prywatności tej grupy zawodowej oraz niepozwalających na rozszerzającą wykładnię pojęć, jest rozwiązaniem pożądanym z punktu widzenia ochrony danych osobowych.

W okresie sprawozdawczym do Biura GIODO skierowano również do zaopiniowania projekt **ustawy o zmianie ustawy o zasadach prowadzenia polityki rozwoju oraz**

niektórych innych ustaw[160]. Powołując na wstępie gwarancje przewidziane przede wszystkim w Konstytucji Rzeczypospolitej Polskiej (art. 31 ust. 3, art. 47), Generalny Inspektor negatywnie ustosunkował się do rozwiązania, zgodnie z którym dane osobowe przetwarzane na potrzeby realizacji programów operacyjnych oraz programów służących realizacji umowy partnerstwa, o ile są wykorzystywane w celu ich realizacji, nie podlegają przepisom o ochronie danych osobowych[161]. Zdaniem Generalnego Inspektora wprowadzenie tego typu ograniczeń praw i wolności jednostki nie spełnia konstytucyjnego kryterium proporcjonalności, tym bardziej wobec zaprezentowanych – jako uargumentowanie celowości wyłączenia przetwarzanych danych osobowych spod jakiejkolwiek ochrony – w treści uzasadnienia przykładów. Ustawodawca wskazał bowiem, że niezbędność wprowadzenia regulacji o takiej treści wynika z faktu, iż, cyt.: *„(...) Stosowanie ustawy o ochronie danych osobowych w kontekście realizacji programów operacyjnych współfinansowanych środkami UE natrafia na szereg praktycznych problemów”*, jak na przykład problem z możliwością upubliczniania wykazu beneficjentów, tytułu operacji i przyznanych im kwot finansowania publicznego, kwestii statusu administratora danych w kontekście istnienia instytucji zarządzającej i pośredniczącej oraz wreszcie problem konieczności nadawania stosownych upoważnień i związane z tym „trudności”. Żaden z przytoczonych przykładów nie powinien stanowić przeszkody w prawidłowej realizacji zadań wynikających z konieczności wywiązywania się przez Rzeczpospolitą Polską z obowiązków wynikających z przepisów unijnych.

Jeżeli chodzi o publikację wykazu beneficjentów należy zaznaczyć, iż przepis upoważniający do powyższego działania został wprowadzony przepisami rangi unijnego rozporządzenia (a więc aktu prawnego obowiązującego na terytorium państw członkowskich i stosowanego w sposób bezpośredni) i została tym samym spełniona przesłanka legalności przetwarzania danych osobowych, o której mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Skoro z przepisu takiego wprost wynika konieczność publikacji, ustawa o ochronie danych osobowych nie stoi na przeszkodzie takiemu działaniu, zaś wskazywanie, że pomimo wszystko obowiązujące przepisy o ochronie danych osobowych na powyższe nie

[160] DOLiS-033-49/13

[161] Proponowana treść art. 32a ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju (Dz. U. z 2009 r. Nr 84, poz. 712 z późn. zm.), tj. art. 1 pkt 21 projektu ustawy o zmianie ustawy o zasadach prowadzenia polityki rozwoju oraz niektórych innych ustaw.

pozwalają, wynika z niezrozumienia idei ochrony danych osobowych oraz systemu prawa jako takiego.

Zgłaszając uwagi do projektu GIODO wskazał jednocześnie, że na gruncie przepisów o ochronie danych osobowych istnieje różnica pomiędzy administratorem danych (art. 7 pkt 4 ustawy o ochronie danych osobowych) oraz podmiotem, któremu przetwarzanie danych osobowych zostało jedynie powierzone (art. 31 ustawy o ochronie danych osobowych). Trudno uznać, iż argumentem przemawiającym za całkowitym pozbawieniem osób, których dane osobowe w taki czy inny sposób stają się przedmiotem przetwarzania w ramach realizacji określonego programu unijnego, może być trudność w określeniu przymiotu administratora danych i uprawnień, które spoczywają na innych podmiotach zaangażowanych w proces rozdysponowywania środków unijnych. Na całkowite pominięcie zasługuje także wskazany w uzasadnieniu argument w zakresie nadawania upoważnień do przetwarzania danych osobowych. Każda osoba dopuszczona do przetwarzania danych osobowych (np. poprzez wgląd do nich) winna legitymować się wydanym przez administratora danych (bądź osobę przez niego upoważnioną) upoważnieniem i Generalny Inspektor w toku dotychczasowej działalności nie spotkał się z sygnałami o nadmiernych trudnościach w dopełnianiu tegoż obowiązku. Wydaje się raczej, iż powyższe pozostaje jedynie kwestią dobrej organizacji.

Odnosząc się zaś do sygnalizowanych przez projektodawcę „problemów z upublicznianiem adresów mailowych pracowników instytucji publicznych zaangażowanych w realizację programów współfinansowanych środkami UE", w pierwszej kolejności zaznaczyć należy, iż takie informacje o pracowniku, jak jego imię i nazwisko, zajmowane stanowisko, służbowy adres e – mail, czy też służbowy numer telefonu są ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. Informacje w tym zakresie mogą być udostępnianie przez pracodawcę – także w przypadku braku zgody osoby, której te dane dotyczą – o ile jest to uzasadnione realizacją przez pracodawcę stosunku zatrudnienia, czy organizacji zakładu pracy (art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych). Na poparcie powyższych stwierdzeń w opinii przytoczony został wyrok Sądu Najwyższego z dnia 19 listopada 2003 r. o sygn. I PK 590/02 *„(...) nazwisko (i imię) jest z natury rzeczy skierowanym na zewnątrz znakiem rozpoznawczym osoby fizycznej i wymienienie go (ujawnienie) przez inny podmiot w celu identyfikacji danej osoby nie może być zasadniczo uznane za bezprawne, o ile ze względu na okoliczności*

towarzyszące nie łączy się to z naruszeniem innego jej dobra, np. czci, godności osobistej lub prywatności." I dalej, cyt.: *„(...) najistotniejszym składnikiem zakładu pracy (przedsiębiorstwa) są ludzie, a funkcjonowanie zakładu wiąże się nierozłącznie z kontaktami zewnętrznymi – z kontrahentami, klientami, administracją publiczną itd. Dlatego pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników zajmujących określone stanowiska w ramach instytucji. Przeciwne stanowisko prowadziłoby do sparaliżowania lub poważnego ograniczenia możliwości działania pracodawcy, bez żadnego rozsądnego uzasadnienia w ochronie interesów i praw pracownika. W normalnym bowiem układzie nie ma racjonalnych powodów, dla których pracownik byłby zainteresowany zachowaniem w tajemnicy swojego nazwiska, a co za tym idzie, faktu związania z danym zakładem pracy. Imiona i nazwiska pracowników widnieją na drzwiach w zakładach pracy, umieszcza się je na pieczątkach imiennych, pismach sporządzanych w związku z pracą, prezentuje w informatorach o instytucjach i przedsiębiorstwach, co oznacza, że zgodnie z powszechną praktyką są one zasadniczo jawne. Nie może to jednak oznaczać nieskrępowanego prawa pracodawcy do ujawniania nazwiska pracownika. Należy przyjąć, że ujawnienie przez pracodawcę nazwiska pracownika musi być usprawiedliwione celem działania pracodawcy, łączącym się z jego zadaniami i obowiązkami związanymi z prowadzeniem zakładu, musi być niezbędne oraz nie może naruszać praw i wolności pracownika (...) Wskazane kryteria znajdują obecnie oparcie w art. 23 ust. 1 pkt 5 ustawy (...) o ochronie danych osobowych (...), jednakże mają one znaczenie ogólniejsze, niezależnie od tego, czy w danej sytuacji istnieją podstawy do stosowania tej ustawy, czy nie. Wyznaczają one bowiem adekwatne i mieszczące się w ramach porządku prawnego przesłanki uzasadniające ujawnianie nazwiska pracownika przez pracodawcę".*

W trakcie prac legislacyjnych zwłaszcza wobec obrony stanowiska w toku konferencji uzgodnieniowej, projektodawcy wykreślili sporny przepis z treści projektu.

Istotny głos w dyskusji Generalny Inspektor zabrał opiniując poselski projekt **ustawy o zmianie ustawy o opiece nad dziećmi w wieku do lat 3**[162], wobec którego przygotowane przez Rząd stanowisko podzieliło obawy GIODO. Projekt przewidywał wprowadzenie monitoringu w placówkach zajmujących się opieką nad dziećmi w wieku do lat 3. Poza

[162] DOLiS-033-137/13

rozwiązaniami *stricte* prawnymi zaproponowano w nim pewne sugestie co do rozwiązań technicznych, które można lub należy zastosować, prowadząc wideonadzór takich placówek.

GIODO w pierwszej kolejności stwierdził, że stosowanie wideonadzoru w proponowanym w projekcie zakresie nie będzie spełniało wyłącznie funkcji kontroli właściwego wypełniania obowiązków przez osoby sprawujące opiekę nad dziećmi w wieku do lat trzech. W wyniku tego typu przedsięwzięcia pozyskiwane będą dane osobowe, które często będzie można zaliczyć do danych wrażliwych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, dotyczące małoletnich, nieświadomych faktu monitorowania ich zachowań, dzieci. Trudno również będzie wprowadzić jakąkolwiek kontrolę nad dowolnym rozpowszechnianiem pozyskanych materiałów przez rodziców, czy innych opiekunów prawnych dzieci, co w przyszłości, może mieć istotne znaczenie zwłaszcza dla ostatniej z wymienionych grup.

Wyrażane przez GIODO wątpliwości dotyczyły kwestii ochrony danych osobowych dzieci, pracowników placówek oraz innych osób znajdujących się na obszarze poddanym wideonadzorowi. W pewnym zakresie odniosły się również do kwestii bezpieczeństwa teleinformatycznego. Generalny Inspektor zwrócił ponadto uwagę, że w dyskusji nad nowelizacją konieczne jest uwzględnienie całości zagadnień ochrony i retencji danych telekomunikacyjnych oraz aspektów prawno-pracowniczych wideonadzoru w zakładzie pracy.

Generalny Inspektor wyraził zasadnicze zastrzeżenia co do podstaw prawnych wprowadzania systemów wideonadzoru w placówkach zajmujących się opieką nad dziećmi w wieku do lat 3, szczególnie w przypadkach, gdy nie można uzyskać dobrowolnej zgody na takie działania ze strony wszystkich osób nim objętych (pracowników placówki, rodziców i opiekunów dzieci oraz osób dopuszczonych do wykonywania różnych czynności na terenie placówki), umożliwienia dostępu online do danych z wideonadzoru, zasad bezpieczeństwa danych zebranych w wyniku działań monitoringu wideo, a także rejestracji zbiorów danych.

Generalny Inspektor zwrócił uwagę, że nie jest możliwe takie pozyskiwanie przez rodziców i opiekunów informacji z wideonadzoru, którego zakres będzie ograniczony wyłącznie do informacji o ich dziecku. Odpowiednie urządzenia rejestrować bowiem będą obraz znajdujący się w polu ich zasięgu. W przypadku dzieci, mogą to być różnego rodzaju zachowania, których ujawnienie mogłoby naruszyć ich prawo do prywatności w sposób zasadniczy, pomijając przy tym inny ważny aspekt wychowawczy, a mianowicie kwestie

zaufania do osób dorosłych. Dlatego też, aby uzyskać cele szeroko opisywane w uzasadnieniu do przedłożonej nowelizacji, w pierwszej kolejności należałoby poddać analizie aktualnie obowiązujące przepisy w zakresie nadzoru nad funkcjonowaniem żłobków, czy klubów dziecięcych i ewentualnie wzmocnić uprawnienia właściwych organów (choćby w zakresie wpływu na kwestie zatrudniania w tych placówkach personelu).

Z proponowanego ust. 1 art. 25a ustawy wynika, iż dyrektor żłobka lub klubu dziecięcego może zainstalować system monitoringu placówki w celu zwiększenia bezpieczeństwa dzieci w niej przebywających. Obowiązek po stronie dyrektora placówki w zakresie wprowadzenia tego typu „systemu kontroli" powstaje zawsze wówczas, gdy o powyższe wystąpi więcej niż połowa rodziców lub opiekunów prawnych dzieci przebywających w tej placówce (projektowany art. 25a ust. 2 ustawy o opiece nad dziećmi w wieku do lat 3). Z tego wynika, iż przedmiotowe rozwiązania dopuszczają sytuacje, kiedy wbrew woli jakiejś części rodziców lub opiekunów prawnych dzieci przebywających w danej placówce, ich dzieci/podopieczni monitoringiem takim zostaną jednak objęte/objęci. Projektodawca przewiduje bowiem pozostawienie tej decyzji albo w rękach dyrektora placówki, niezależnie od woli rodziców czy opiekunów prawnych, albo w rękach co najmniej połowy tej grupy osób. Opiniowana regulacja dopuszcza zatem wprowadzenie istotnych ograniczeń konstytucyjnych praw jednostki, która jest małoletnim dzieckiem, bez aprobaty osób najbardziej związanych z nimi emocjonalnie, a być może nawet pomimo ich wyraźnego sprzeciwu, przedstawicieli ustawowych – osób odpowiedzialnych w pierwszej kolejności za właściwy rozwój dzieci. Bezsprzecznie natomiast rodzice lub opiekunowie prawni dzieci, którzy są świadomi negatywnych konsekwencji wynikających z samego faktu prowadzenia wideonadzoru dzieci, a także ujawnienia osobom postronnym materiałów pochodzących z nagrań zgromadzonych za jego pomocą, powinni mieć prawo do zadecydowania w tym przedmiocie, zgodnie z własnym przekonaniem.

Analiza legalności doprowadziła do przywołania w pierwszej kolejności przepisów Konstytucji RP, tj. w szczególności art. 31 ust. 3 i art. 47.

Generalny Inspektor stwierdził, że stosowanie technologii wideonadzoru, w której rejestrowane będą niedające się dookreślić z góry zachowania dzieci w wieku do lat 3 (a także ich opiekunów) stanowi głęboką ingerencję w prawo do prywatności tychże osób. Przedstawiając argumentację, powołał się także na przyjętą w dniu 11 lutego 2004 r. Opinię 4/2004 Grupy roboczej do spraw ochrony osób fizycznych w zakresie przetwarzania danych

osobowych[163] (GR Art. 29), w której zwrócono uwagę, że o ile w niektórych przypadkach wideonadzór daje się usprawiedliwić, w innych mamy do czynienia z impulsywnym sięganiem po techniki ochrony z użyciem kamer, bez odpowiedniego zastanowienia się nad warunkami i sposobami ich użycia. W dalszej części opinii GR Art. 29 stwierdziła, cyt.: *„(...) Nadmierne rozpowszechnianie systemów pozyskiwania obrazu w miejscach publicznych i prywatnych nie może spowodować nieuzasadnionego ograniczenia podstawowych praw i wolności obywateli, w przeciwnym razie mogliby być zmuszeni podporządkować się w nieproporcjonalny sposób procedurom gromadzenia danych, które czyniłyby ich masowo identyfikowalnymi w dużej liczbie miejsc publicznych i prywatnych (...)”*.

W niniejszej opinii, którą biorą pod uwagę także inne państwa członkowskie Europejskiego Obszaru Gospodarczego (EOG), wskazano m.in. na konieczność respektowania zasady proporcjonalności przy posługiwaniu się wideo nadzorem - dane muszą być adekwatne i istotne dla celów przetwarzania. Zasada ta oznacza przede wszystkim, że urządzenia wideonadzoru mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być zastosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, nie wymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami.

Organ do spraw ochrony danych osobowych negatywnie ustosunkował się natomiast do samej idei udostępniania obrazu i dźwięku w Internecie, za pomocą zestawu kodów dostępu uprawniających w czasie rzeczywistym do podglądu w sieci danych z monitoringu. Wprowadzenie takiego rozwiązania, zwłaszcza że nagrania będą utrwalane, a dyrektor placówki na każde żądanie rodziców będzie miał obowiązek ich udostępniania, jest niepoproporcjonalne w stosunku do ewentualnych korzyści z monitorowania. Wrażliwość informacji, która miałaby być dostępna przez Internet oraz realne zagrożenie „przechwycenia” tak transmitowanego obrazu audiowizualnego wobec braku skutecznych mechanizmów bezpieczeństwa, a tym samym negatywne konsekwencje po stronie osób objętych wideonadzorem, w kontekście wyżej powołanych przepisów sprzeciwiają się zastosowaniu tego typu rozwiązania.

[163] Ciało opiniodawczo-doradcze powołane na podstawie art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.95.281.31).

W kwestii zasad bezpieczeństwa danych zebranych w wyniku działań wideo nadzorczych GIODO wskazał na zbędności odwoływania się do przepisów ustawy o ochronie danych osobowych[164]. Ustawa ta jest bowiem aktem prawnym powszechnie obowiązującym i jej stosowanie pozostaje koniecznością bez względu na wprowadzanie innych przepisów do niej się odwołujących. Podkreślenia jednak wymaga, że wobec takiego ukształtowania treści przepisów pojawić się może pytanie, co w sytuacji, gdy inne ustawy nie zawierają stosownego odesłania, tj. czy powyższe oznaczać ma zwolnienie z obowiązku stosowania przepisów o ochronie danych osobowych w materii objętej treścią danego aktu prawnego.

Istotne jest natomiast pominięcie regulacji dotyczących zasad zabezpieczania infrastruktury informatycznej, która w przypadku proponowanego ustawą rozstrzygnięcia – szczególnie przy przyjęciu krytykowanego powyżej dostępu online do zbioru – będzie wykazywać inne elementy ryzyka niż klasyczne systemy gromadzące dane osobowe. Tym samym proponowane brzmienie delegacji ustawowej w zakresie wprowadzenia delegacji dla ministra właściwego do spraw informatyzacji[165], powinno zostać uzupełnione o konieczność określenia również sposobów zabezpieczenia tej części infrastruktury informatycznej (oprogramowania i elementów fizycznych), na których odbywa się proces przetwarzanie danych osobowych.

Uznając informacyjny walor przepisów dotyczących rejestracji zbiorów w rejestrze prowadzonym przez GIODO, organ do spraw ochrony danych osobowych wskazał na zbędność wprowadzania w projekcie obowiązku zgłaszania zbiorów danych osobowych. Sama bowiem ustawa o ochronie danych osobowych przesądziła, iż wobec braku zaistnienia wyjątku od zasady zgłaszania zbiorów danych do rejestracji przez ich administratorów, istnieje konieczność zgłoszenia zbiorów „nieobjętych wyłączeniem" organowi do spraw ochrony danych osobowych[166]. Co więcej, takie powtórzenie sugeruje, że bez wprowadzenia przepisu do ustawy obowiązek by nie istniał, co po prostu nie jest prawdą.

Za rezygnacją z treści proponowanego brzmienia art. 25b ustawy przemawia również okoliczność, iż ustawa o ochronie danych osobowych stanowi o zgłaszaniu do rejestracji

[164] Projektowany art. 25b ust. 2 ustawy o opiece nad dziećmi w wieku do lat 3.
[165] Projektowany art. 25a ust. 6 ustawy o opiece nad dziećmi w wieku do lat 3.
[166] Zgodnie z art. 40 ustawy o ochronie danych osobowych, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

zbiorów danych osobowych w rozumieniu jej art. 7 pkt 2[167]. Zakres przedmiotowy art. 40 ustawy o ochronie danych osobowych nie obejmuje natomiast przetwarzania danych osobowych poza zbiorem, np. w systemie informatycznym. Z przedłożonego projektu[168] wynika natomiast, że system monitoringu może (a więc nie musi) składać się z urządzeń rejestrujących obraz i dźwięk, które mogą być (czyli nie muszą) utrwalane i przechowywane na nośnikach pamięci przez okres nie dłuższy niż 90 dni, a następnie niszczone. Generalny Inspektor wskazał więc, że nie każde przetwarzanie danych poprzez system monitoringu będzie, z punktu widzenia ustawy o ochronie danych osobowych, kwalifikować się do zgłoszenia do rejestracji jako zbiór danych.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych opiniował również projekt **ustawy o zmianie ustawy – Prawo o szkolnictwie wyższym oraz niektórych innych ustaw[169]**, który dotyczył m.in. monitoringu karier zawodowych absolwentów[170], w tym także przetwarzania danych w Systemie Informacji o Szkolnictwie Wyższym w ramach Zintegrowanego Systemu Informacji o Nauce i Szkolnictwie Wyższym „POL – on"[171].

GIODO w pierwszej kolejności podkreślił, że w demokratycznym państwie prawnym urzeczywistniającym zasady sprawiedliwości społecznej (art. 2 Konstytucji RP) dla uznania legalności rozwiązań ingerujących w sferę prywatności jednostki nie wystarczy ich ustawowy charakter, konieczne jest bowiem wykazanie ich niezbędności (art. 31 ust. 3 i art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej[172]). Wyrażając uwagi do proponowanych rozwiązań, Generalny Inspektor nie kwestionował potrzeby dostępności rzetelnych, obiektywnych i porównywalnych danych statystycznych na temat losów zawodowych absolwentów, zwłaszcza dla opinii publicznej i kandydatów na studia. Rozumie bowiem, jak ważne dla

[167] W świetle tego przepisu, zbiorem danych osobowych jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
[168] Proponowane brzmienie art. 25a ust. 4 ustawy o opiece nad dziećmi w wieku do lat 3.
[169] DOLiS-033-318/13
[170] Art. 1 pkt 16 przedłożonego projektu dodający art. 13b do ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym – t.j. Dz. U. z 2012 r. poz. 572 z późn. zm.).
[171] Proponowany art. 34a ustawy - Prawo o szkolnictwie wyższym.
[172] Powołany został w stanowisku wyrok Trybunału Konstytucyjnego z dnia 20 listopada 2002 r. o sygn. akt K 41/02 Trybunał wskazał, że istnienie w przedmiotowym przepisie odrębnej regulacji dotyczącej proporcjonalności wkraczania w prywatność jednostki należy tłumaczyć tym, iż naruszenie autonomii informacyjnej poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce, jest typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki.

młodego człowieka w podejmowaniu decyzji w zakresie wyboru dalszego kierunku kształcenia są obiektywne dane na temat perspektywy jego losów zawodowych, możliwości zatrudnienia oraz zarobkowania. Niemniej jednak powyższych założeń nie można realizować w oderwaniu od poszanowania prawa do prywatności jednostki i w konsekwencji przy użyciu środków dotkliwie ingerujących w to gwarantowanie konstytucyjnie prawo, nadmiernych i zwyczajnie zbędnych z punktu widzenia realizacji celu (art. 47 Konstytucji RP). Dlatego też jako wymagające rozważenia wskazał na zakres danych osobowych przekazywanych do Zakładu Ubezpieczeń Społecznych oraz zapewnienia pełnej anonimowości przekazywanych przez ZUS danych z powrotem do ministra właściwego ds. szkolnictwa wyższego, a także konieczność prowadzenia ww. monitoringu karier nie tylko przez uczelnie wyższe – każda w zakresie swoich absolwentów – ale, jak się planuje, przez ww. ministra.

Przede wszystkim GIODO zanegował przepis projektowanej ustawy, zgodnie z którym „uczelnia może prowadzić własny monitoring karier zawodowych absolwentów i w tym celu przetwarzać może imiona i nazwisko, adres zamieszkania lub adres zameldowania lub adres do korespondencji, numer telefonu oraz adres poczty elektronicznej”[173]. Wskazał też, że nie powinno dochodzić do sytuacji nakładania na absolwentów obowiązku posiadania poczty elektronicznej oraz wyraził sprzeciw wobec uprawnienia podmiotów, które dysponują dostępem do danych osób pobierających naukę na uczelniach wyższych, do podejmowania działań monitorujących znaczną część ich życia z pomocą bliżej nieokreślonych narzędzi. Generalny Inspektor stwierdził, że zaproponowany system „podwójnego systemu śledzenia losów absolwentów” – tak na szczeblu centralnym, jak i z poziomu poszczególnych uczelni wyższych – rodzi nadmierną i nieadekwatną do celu ingerencję w prywatność i prowadzi do utraty przez podmioty danych kontroli nad procesem przetwarzania ich danych osobowych. Wobec brzmienia art. 170c aktualnie obowiązującej ustawy – Prawo o szkolnictwie wyższym[174], wydaje się, iż to minister właściwy do spraw szkolnictwa wyższego powinien być podmiotem posiadającym wyłączne prawo prowadzenia wspominanego monitoringu.

Generalny Inspektor pod rozwagę poddał zasadność przekazywania Zakładowi Ubezpieczeń Społecznych przez ministra właściwego do spraw szkolnictwa wyższego informacji o absolwentach na temat: nazwy uczelni, nazwy jednostki prowadzącej studia,

[173] Dodawany art. 13b ust. 9 i 10 ustawy - Prawo o szkolnictwie wyższym.
[174] Zgodnie z tym przepisem minister właściwy do spraw szkolnictwa wyższego prowadzi ogólnopolski wykaz studentów; zakres danych określono w ust. 2 przepisu i wskazano m.in. na imię i nazwisko studenta, numer PESEL, czy rodzaj przyznanych mu świadczeń pomocy materialnej w uczelni.

formy studiów oraz kierunku, poziomu i profilu kształcenia, roku i miesiąca rozpoczęcia studiów oraz roku i miesiąca ich ukończenia. Powstaje bowiem pytanie, czy celem przekazania informacji o absolwentach jest ich uzupełnienie przez ZUS o informacje dotyczące „przybliżonego obszaru zawodowego", w którym absolwenci pracują, a także tego samego rodzaju informacje w zakresie osiąganych dochodów, oraz następcze dokonanie agregacji danych i ich przekazanie do ministra, czy też stworzenie również przez ZUS bazy danych o absolwentach. Zdaniem GIODO, aby osiągnąć założenia prezentowane także w uzasadnieniu do projektu, wystarczającym byłoby przekazanie do ZUS informacji pozwalających jedynie na ustalenie tożsamości osoby fizycznej. Z tego punktu widzenia już sam numer PESEL uzupełniony – celem wyeliminowania ewentualnych wątpliwości czy błędów – o imię i nazwisko absolwenta, spełniałby dostatecznie funkcję identyfikacyjną. GIODO stwierdził, że brak jest przesłanek, aby ZUS wchodził w posiadanie informacji o kończonej przez daną osobę uczelni, a także w przedmiocie formy studiów, czy dat ich rozpoczęcia i zakończenia.

Uwzględniając ilość i charakter danych przekazywanych przez ZUS ministrowi właściwemu do spraw szkolnictwa wyższego, GIODO poddał w wątpliwość możliwość zapewnienia ich pełnej anonimizacji i braku możliwości dopasowania przez „pierwotnego" administratora danych przekazanych rekordów do konkretnych osób fizycznych. Zdaniem GIODO wystarczającym byłoby ilościowe ujęcie przekazywanych danych bez nadawania im jakiegokolwiek zindywidualizowanego charakteru (choćby poprzez kod osoby ubezpieczonej wygenerowany przez ZUS). Dla uzyskania informacji o ścieżce zawodowej absolwentów danej uczelni, celem ich przekazania społeczeństwu dla oceny przydatności danego kierunku kształcenia dla życia zawodowego, wystarczająca wydaje się informacja statystyczna. Istotnym jest bowiem, jaka liczba absolwentów danego kierunku pracuje w określonej „branży" oraz jaki jest przedział osiąganych przez nich z tego tytułu dochodów.

GIODO wskazał ponadto, że przedłożona propozycja regulacji pominęła w zupełności kwestie przechowywania przez ZUS danych pozyskanych od ministra oraz zmian w zakresie zadań aktualnie wykonywanych przez ten organ, na podstawie właściwych przepisów prawa.

Odnosząc się zaś do systemu „POL-on" Generalny Inspektor wyraził sprzeciw wobec jego rozszerzania o kolejnego rodzaju dane osobowe dotyczące tak nauczycieli akademickich i pracowników naukowych, jak i studentów (w tym studentów studiów doktoranckich),

a także wprowadzanie podstaw prawnych do tworzenia kolejnych wykazów zawierających dane osobowe określonych grup osób.

Ustawodawca w projekcie przewidział rozszerzenie dotychczas przetwarzanego – i tak już dość szerokiego – zakresu danych osobowych, które przetwarzane są w ramach systemu nauki, w tym przez ministra właściwego do spraw szkolnictwa wyższego[175]. Proponuje się także dodanie przepisów materialnych dających ministrowi podstawę do prowadzenia ogólnopolskiego wykazu słuchaczy studiów podyplomowych, wykazu doktorantów, czy osób, którym nadano stopień doktora i doktora habilitowanego, tytuł profesora, a także ogólnopolskiej bazy streszczeń i recenzji rozpraw doktorskich oraz autoreferatów i recenzji w postępowaniach habilitacyjnych, według obszaru wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych. Abstrahując od realnej potrzeby władania przez ministra tymi informacjami, Generalny Inspektor wyraził zdziwienie wynikającym z projektu dążeniem tego organu do władania tak szerokim zakresem informacji o wielu milionach osób. Wskazał na fakt, iż posiadanie statusu administratora danych osobowych względem zbioru danych o takich rozmiarach niesie za sobą szereg obowiązków, a z wywiązywaniem się z nich – uwzględniając spectrum proponowanych rozwiązań – mogą istnieć stosunkowo duże problemy. Powstaje bowiem pytanie, czy minister będzie realizował np. wnioski o uzupełnienie, uaktualnienie, sprostowanie, czy usunięcie danych, składane przez osoby, których dane te dotyczą, a jeżeli nie, to w oparciu o jakie przepisy.

Na uwagę zasługuje również stanowisko przedstawione przez Generalnego Inspektora Ochrony Danych Osobowych wobec projektu **ustawy o zasadach realizacji programów operacyjnych polityki spójności finansowanych w perspektywie finansowej 2014 – 2020**[176].

Generalny Inspektor zakwestionował przepis dotyczący kryteriów, jakie musi spełnić osoba pełniąca funkcję eksperta[177], z uwagi na użyte w nim lapidarne określenie „inne wymogi określone przez właściwą instytucję", które powoduje wątpliwości interpretacyjne i może prowadzić do naruszenia zasady adekwatności danych w stosunku do celu ich

[175] W przepisach projektu proponuje się rozszerzenie zakresu danych m.in. o dane dotyczące kraju pochodzenia danej osoby, kraju wydania dokumentu tożsamości, jej roku urodzenia, płci, tytule zawodowym, stopniu naukowym lub tytule naukowym, miejscu stałego zameldowania przed rozpoczęciem studiów - m.in. proponowany art. 129a ust. 2, czy art. 170c ust. 2 ustawy - Prawo o szkolnictwie wyższym.
[176] DOLiS-033-417/13
[177] Art. 39 ust. 2 pkt 5 projektu

przetwarzania[178]. Analogiczne powody stanęły za postulatem doprecyzowania brzmienia przepisu dotyczącego wnoszonego w formie pisemnej protestu[179].

Zasadnicze uwagi organu do spraw ochrony danych osobowych dotyczyły rozdziału 15 projektu, w którym nie zostały dookreślone zasady funkcjonowania centralnego systemu teleinformatycznego wspierającego realizację programów operacyjnych. GIODO zaznaczył, że nie neguje potrzeby posługiwania się takim sposobem wymiany informacji, który m.in. przyspieszy realizację poszczególnych programów unijnych, ograniczy obciążenia administracyjne czy zlikwiduje bariery w dostępie do pomocy poprzez racjonalizację i standaryzację procesów. Niemniej jednak tym sposobem powstanie kolejna już megabaza danych o osobach fizycznych. Uwzględniając przy tym, iż regulacje unijne, które nakazują państwom członkowskim zapewnienie funkcjonowania systemu informatycznego, za pomocą którego odbywać się będzie pełna komunikacja między beneficjentami a właściwymi instytucjami nie zostały jeszcze przyjęte[180], GIODO wskazał, że kwestie zapewnienia właściwego poziomu ochrony danych osobowych, które mają być przetwarzane w przedmiotowym systemie teleinformatycznym, wymagają głębokiej analizy ze strony projektodawców. Na każdym etapie planowania rozwiązań, które prowadzą do tworzenia baz danych zawierających niezliczone rekordy, i które są prowadzone za pomocą systemu teleinformatycznego, rozważać należy ich wpływ na sferę prywatności (tzw. koncepcja *privacy by design*). Powyższa koncepcja zakłada, iż najważniejsze problemy związane z ochroną prywatności w kontekście funkcjonowania podobnych systemów należy przewidywać już na etapie poprzedzającym ich budowę – od samego początku aż po zakończenie, a więc – co istotne – jeszcze przed rozpoczęciem pozyskiwania i dalszego przetwarzania danych osobowych. Powyższe umożliwia bowiem podejmowanie odpowiednich działań ukierunkowanych na zapobieganie występowaniu przedmiotowych problemów, zamiast następczego reagowania na pojawiające się nieprawidłowości.

---

[178] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych oraz art. 6 ust. 1 lit. c dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.WE.23.11.1995).

[179] Art. 42 ust. 2 pkt 2 projektu.

[180] Projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego objętych zakresem wspólnych ram strategicznych oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego i Funduszu Spójności, oraz uchylającego rozporządzenie (WE) nr 1083/2006.

Wynik przedmiotowych rozważań powinien znaleźć swe odzwierciedlenie we właściwie skonstruowanych przepisach aktu prawnego rangi ustawy. Tak więc wszelkie zasady funkcjonowania opisywanego systemu, w tym w szczególności zakres przetwarzanych w nim danych, prawa dostępu do jego zasobów, czy ewentualne uprawnienie do cedowania kompetencji w zakresie administrowania jego zasobami na inny podmiot, powinno zostać uregulowane na szczeblu aktu ustawowego.

Tymczasem projektodawca z jednej strony dostrzega przełom, jaki projektuje ustawodawca unijny w związku z przetwarzaniem danych w ramach programów operacyjnych, stanowiąc w treści uzasadnienia o „olbrzymiej rewolucji w procesie wdrażania funduszy unijnych", z drugiej jednak, wprowadzając kilka lapidarnie brzmiących przepisów, mnoży wątpliwości. Powstaje np. pytanie, jaki zakres danych należy rozumieć pod pojęciem „ewidencjonowania danych dotyczących programów operacyjnych"[181]; czy wystarczającą gwarancję zapewnienia właściwego poziomu ochrony przetwarzanym w planowanym systemie danym osobowym stanowić ma możliwość uwierzytelnienia w tym systemie za pomocą profilu zaufanego e-PUAP lub poprzez bliżej niedookreślone wykorzystanie loginu i hasła „wygenerowanego przez system"; co oznacza możliwość „przetwarzania" danych osobowych, których „administratorem jest inny podmiot" przez instytucję zarządzającą oraz wreszcie, czy wystarczającym powodem uznania ministra właściwego do spraw rozwoju regionalnego za administratora danych zgromadzonych w systemie jest – co wynika z treści uzasadnienia[182] – uczynienie go odpowiedzialnym za budowę i funkcjonowanie systemu informatycznego[183]. Ponadto podniesione zostało pytanie, czy organ ten ma być jednocześnie tzw. „administratorem systemu informatycznego".

Mimo podtrzymywania stanowiska, także na konferencji uzgodnieniowej z udziałem GIODO, nie wniesiono innych zasadniczych uwag dotyczących centralnego systemu teleinformatycznego, który ma wspierać realizację programów unijnych. Wykreślono jedynie przepis, z którego wynikało, iż instytucja zarządzająca w celu realizacji zadań w zakresie zapewnienia aktualności danych, ustalania korekt finansowych i odzyskiwania kwot podlegających zwrotowi na zasadach wynikających z ustawy o finansach publicznych, może „przetwarzać dane, których administratorem jest inny podmiot" oraz przepis, z którego

[181] Art. 59 ust. 2 pkt 3 projektu.
[182] Str. 25 uzasadnienia do projektu.
[183] Art. 59 ust. 3 projektu.

wynikało, że w takim przypadku administrator danych osobowych powierza dane osobowe w zakresie niezbędnym dla realizacji zadań.

W okresie sprawozdawczym Generalny był mocno zaangażowany w prace legislacyjne nad nowelizacją ustawy o promocji zatrudnienia i instytucjach rynku pracy, najpierw na etapie prac nad **projektem założeń projektu ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw**[184], a następnie nad **rządowym projektem ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy**[185]. W ramach tych prac Generalny Inspektor nie tylko prowadził pisemną korespondencję, ale także uczestniczył w szeregu spotkań poświęconych materii nowelizacji, w tym w roboczych spotkaniach uzgodnieniowych, Komisji Prawniczej, a także w posiedzeniach podkomisji i komisji sejmowych.

Przedłożony do zaopiniowania projekt założeń zawierał propozycję rozszerzenia zakresu tworzonych rejestrów centralnych o dane dotyczące wykonywania pracy przez cudzoziemców[186]. Zmiana w zakresie przepisu dotyczącego rejestrów centralnych prowadzonych przez ministra właściwego do spraw pracy, stała się okazją do przedstawienia pewnych generalnych uwag w tym zakresie, w szczególności ze względu na ogólny charakter norm prawnych, w oparciu o które minister może prowadzić ww. rejestry centralne[187]. W pierwszej kolejności Generalny Inspektor wskazał, że powoływanie do życia rejestrów centralnych musi być uzasadnione celem i jego niezbędnością w demokratycznym państwie prawnym. Przetwarzanie danych osobowych w ramach takich rejestrów stanowi bowiem ingerencję w konstytucyjnie chronione prawo do prywatności (art. 47 Konstytucji RP), którego ograniczenie 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, a ograniczenie to nie narusza istoty wolności i praw (art. 31 ust. 3 Konstytucji

[184] DOLiS-033-70/13
[185] DOLiS-033-529/13
[186] Zmiana w art. 4 ust. 4 ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (tj. Dz. U. z 2013 r. poz. 674 z późn. zm.) - propozycja zawarta w rozdziale VII pkt 2 lit. b projektu założeń.
[187] Zgodnie z art. 4 ust. 4 ustawy o promocji zatrudnienia i instytucjach rynku pracy - w brzmieniu obowiązującym w momencie nadesłania do zaopiniowania - minister właściwy do spraw pracy może tworzyć rejestry centralne zawierające dane dotyczące rynku pracy, instytucji rynku pracy, projektów, udzielonej pomocy i świadczeń, a także dane dotyczące poszukujących pracy, bezrobotnych, pracodawców i ofert pracy, gromadzone przez publiczne służby zatrudnienia na podstawie przepisów ustawy, oraz może przetwarzać te dane na zasadach określonych w przepisach o ochronie danych osobowych.

Rzeczypospolitej Polskiej). Generalny Inspektor podkreślił także konieczność zapewnienia, aby rejestry centralne tworzone były w oparciu o wystarczająco precyzyjne przepisy prawa.

Tymczasem tak obowiązujące przepisy, jak i projektowana zmiana nie udzielają odpowiedzi na zasadnicze pytanie o cel stworzenia rejestru na poziomie centralnym, jak również zasady jego prowadzenia przez ministra właściwego do spraw do spraw pracy, który w związku z tym stanie się *de facto* jego administratorem – w tym danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych – obciążonym szeregiem obowiązków wynikających z przepisów o ochronie danych osobowych. Ponadto z regulacji o randze ustawy w sposób niebudzący wątpliwości wynikać winny kwestie o tak fundamentalnym znaczeniu dla funkcjonowania rejestru na poziomie centralnym, jak: zasady udostępniania (w szczególności, jakim podmiotom miałyby one być udostępniane) i pozyskiwania danych, okres przechowywania zawartych w tym rejestrze danych, zasady ich aktualizowania oraz zasady bezpieczeństwa, jak również kwestia, czy przekazaniu przez publiczne służby zatrudnienia podlegałyby wszystkie gromadzone przez nie dane, czy też dane w bardziej ograniczonym zakresie. Jednocześnie GIODO zaznaczył, że konieczność uregulowania zasadniczych zagadnień merytorycznych w przepisach ustawy nie wyklucza możliwości uszczegółowienia tych kwestii w przepisach rozporządzenia. W ramach uwag szczegółowych organ odniósł się także do zmiany definicji bezrobotnego, zaproponowanej przez projektodawcę jako „ dostosowanie do przepisów 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.), znoszącej instytucję na pobyt stały lub czasowy”[188]. GIODO podkreślił, iż obowiązek zameldowania na pobyt stały lub czasowy w aktualnym stanie prawnym nadal istnieje[189], a z uwagi na dość odległy moment ewentualnej likwidacji tej instytucji, zmiana definicji bezrobotnego nie wydaje się do końca zasadna.

Ustosunkowując się do postulatów GIODO dotyczących rejestrów centralnych projektodawcy wskazywali, że zakres przetwarzanych, w tym gromadzonych,

[188] Rozdział VIII pkt 1 lit. a projektu założeń

[189] Aktem prawnym znoszącym ten obowiązek jest inna ustawa, której termin wejścia w życie był już dwukrotnie przesuwany, tj. *ustawa z dnia 24 kwietnia 2010 r. o ewidencji ludności* (Dz. U. z 2010 r. Nr 217, poz. 1427, z późn. zm.) i w momencie przygotowywania opinii, tj. w marcu 2013 r. jest on wyznaczony na dzień 1 stycznia 2015 r., z wyjątkiem art. 62, który wszedł w życie z dniem 1 stycznia 2013 r. Ponadto mocą art. 5 pkt 9 ustawy z dnia 7 grudnia 2012 r. o zmianie ustawy o ewidencji ludności i dowodach osobistych oraz niektórych innych ustaw (Dz. U. z 2012 r. poz. 1047) została do niej wprowadzona zmiana dotycząca terminu zniesienia obowiązku meldunkowego, polegająca na zmianie daty zniesienia obowiązku meldunkowego z 1 stycznia 2014 r. na datę 1 stycznia 2016 r.

w przedmiotowym rejestrze centralnym danych, czy też zasady jego prowadzenia, są tożsame z zakresem danych bądź sposobem prowadzenia, obsługiwanym przez powiatowe urzędy pracy rejestrze osób bezrobotnych i poszukujących pracy[190]. Już w chwili obecnej z przepisów wynika katalog danych, jaki będzie przez ministra właściwego do spraw pracy przetwarzany, a z roli ministra właściwego do spraw pracy jako koordynatora publicznych służb zatrudnienia[191] i zakresu realizowanych przez niego zadań[192] wynika, że rejestr centralny jest niezbędnym elementem systemu obsługi rynku pracy. Generalny Inspektor w odpowiedzi wskazywał, że choć funkcjonowanie obu rejestrów jest ze sobą powiązane[193], to rejestry te nie są ze sobą tożsame. W szczególności różni będą administratorzy danych tych zbiorów. W przypadku rejestru bezrobotnych i poszukujących pracy o celach i środkach decydować będą, na podstawie i w granicach prawa, powiatowe urzędy pracy. Natomiast w odniesieniu do rejestrów centralnych podmiotem tym będzie minister właściwy do spraw pracy. Jeśliby przyjąć tożsamość obu rejestrów – czy to w zakresie celu ich istnienia, czy katalogu gromadzonych tam informacji – oznaczałoby to zezwolenie na multiplikowanie procesów przetwarzania danych konkretnej osoby, jak i liczby podmiotów przetwarzających te dane. Takiego zaś stanu rzeczy organ do spraw ochrony danych osobowych nie może zaakceptować, gdyż sprzeciwiałoby się to standardowi „niezbędności w demokratycznym państwie prawnym". GIODO stwierdził także, że skoro ustawodawca odrębnie odnosi się do problematyki rejestracji bezrobotnych i poszukujących pracy, w tym do rejestru tych osób, zamieszczając te zagadnienia w rozdziale 9 ustawy o promocji zatrudnienia i instytucjach rynku pracy, i doprecyzowując je w rozporządzeniu w sprawie rejestracji bezrobotnych i poszukujących pracy[194], to tym bardziej należy oczekiwać, że kompleksowo ureguluje problematykę tworzenia i funkcjonowania rejestrów prowadzonych na szczeblu centralnym.

Organ do spraw ochrony danych osobowych przestrzegł również autorów projektu, aby w rozważaniach na temat koncepcji rejestrów centralnych wzięli także pod uwagę zagrożenia związane z istnieniem tak dużego zbioru danych, jak i pokusą ich wykorzystywania dla innych celów aniżeli te, dla których pierwotnie zostały zebrane. Nie można przecież wykluczyć takiej zmiany prawa w przyszłości, która dopuści wykorzystywanie w innym celu

[190] Rejestr prowadzony na podstawie art. 33 ust. 1 ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[191] Art. 5 ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[192] Art. 4 ust. 1 pkt 2 lit. c i pkt 8 ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[193] Z art. 4 ust. 5 ustawy o promocji zatrudnienia i instytucjach rynku pracy wynika, że rejestr centralny ma być zasilany danymi przez publiczne służby zatrudnienia.
[194] Rozporządzenie z dnia 12 listopada 2012 r. (Dz. U. z 2012 r. poz. 1299).

danych zgromadzonych w rejestrze centralnym. Istotnym zagadnieniem była również potencjalna możliwość łączenia systemów teleinformatycznych obsługujących tę bazę z istniejącymi dziś innymi systemami teleinformatycznymi. Ewentualne błędy popełnione dziś przy tworzeniu podstaw prawnych dla przetwarzania danych, mogą w tej sytuacji ciążyć nad działaniem innych systemów w naszym kraju. Generalny Inspektor na poparcie tych twierdzeń przytoczył przykład aktu prawnego, w tworzeniu którego brał udział, dążąc do stworzenia kompleksowych i wystarczająco precyzyjnych podstaw prawnych funkcjonowania innego rejestru centralnego w systemie oświaty, tj. ustawę o systemie informacji oświatowej[195].

Ponadto Generalny Inspektor zwrócił uwagę na zagadnienie udostępniania danych z rejestru centralnego, które miałoby następować na rzecz szerokiego katalogu podmiotów, w tym pomiotów prowadzących badania i analizy rynku pracy[196]. Z uwagi na różnorodność podmiotów, o których mowa w proponowanym art. 4 ust. 6 ustawy o promocji zatrudnienia i instytucjach rynku pracy, GIODO wskazał na potrzebę stworzenia kilku norm, które precyzyjnie określiłyby zasady dostępu do rejestrów centralnych. Zasady tego udostępniania powinny uwzględniać różny charakter podmiotów, na rzecz których następuje udostępnienie oraz przyświecające mu cele. Zaproponowana norma w jednym rzędzie umieściła zarówno publiczne służby zatrudnienia, inne podmioty realizujące zadania na podstawie ustawy lub odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny, jak i podmioty prowadzące badania i analizy rynku pracy na zlecenie publicznych służb zatrudnienia. Dla tej pierwszej grupy podmiotów udostępnianie miało być ograniczone do zakresu danych niezbędnych do realizacji tych zadań, w odniesieniu zaś do drugiej kategorii podmiotów sformułowano cel udostępnienia, tj. ocenę skuteczności udzielanej pomocy lub poprawy ich funkcjonowania, lecz nie wskazano jego zakresu.

[195] Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (tj. Dz. U. z 2011 r. Nr 139, poz. 814 z późn. zm.). W toku prac nad projektem – również na skutek postulatów GIODO – przyjęte zostały szczegółowe regulacje prawne odnoszące się do szeregu istotnych – z perspektywy procesu przetwarzania danych osobowych – zagadnień dotyczących bazy danych Systemu Informacji Oświatowej (centralnego zbioru danych), zwanego dalej SIO, prowadzonej przez ministra właściwego do spraw oświaty i wychowania. Rozwiązania zawarte w przepisach tejże ustawy określają mianowicie m.in.: rodzaj i zakres danych osobowych gromadzonych w SIO (rozdział 2), przekazywanie danych do bazy danych SIO (rozdział 3), pozyskiwanie danych dziedzinowych z bazy danych SIO (rozdział 4), dostęp do bazy danych SIO (rozdział 5), nadzór nad bezpieczeństwem przekazywania danych do bazy danych SIO i pozyskiwania danych z bazy danych SIO (rozdział 6).

[196] Projektowany art. 4 ust 6 ustawy o promocji zatrudnienia i instytucjach rynku pracy.

Ponadto zaproponowana konstrukcja skłoniła do postawienia pytania o uzasadnienie dla zrównania uprawnień podmiotów prowadzących badania i analizy rynku pracy, z uprawnieniami publicznych służb zatrudnienia i innych podmiotów realizujących zadania na podstawie ustawy lub odrębnych przepisów. Publiczne służby zatrudnienia lub inne podmioty działające na podstawie przepisów wypełniają nałożone przez ustawodawcę obowiązki, a ich dostęp do określonych danych jest ściśle powiązany z wypełnianiem tych zadań. Są to więc podmioty objęte reżimem działania jedynie na podstawach i w granicach prawa[197]. Natomiast nie do końca jasne jest, z czego wywodzić należy uprawnienie podmiotów prowadzących badania i analizy rynku pracy do dostępu do rejestru centralnego, i to dostępu do całości zasobów przetwarzanych w rejestrze centralnym. Zasadnym byłoby zastanowienie się, czy realizacja obowiązku prowadzenia badań i analiz rynku pracy powinna następować przez podmioty trzecie, niebędące publicznymi służbami zatrudnienia. Jeżeli odpowiedź na to pytanie byłaby pozytywna, to z przepisów prawa wynikać powinno ewentualne uprawnienie do dostępu do określonych zasobów informacyjnych w zakresie niezbędnym do wypełnienia przedmiotowego obowiązku. Nie wydaje się właściwe, aby zezwolenie na dostęp do tak ogromnego zbioru danych, jak rejestr centralny, mogło wynikać jedynie z umowy zlecenia na badania i analizy rynku pracy. Taka forma nie może zostać uznana za zapewniającą odpowiednie gwarancje ochrony danych przetwarzanych w rejestrze centralnym, zwłaszcza jeśli udostępnianiu miałyby podlegać dane szczególnie chronione. Zapewnienie odpowiedniego poziomu ochrony może zostać natomiast osiągnięte w odpowiednio skonstruowanych normach powszechnie obowiązującego prawa.

W posumowaniu GIODO wskazał, że uprawnienie podmiotów prowadzących badania i analizy rynku pracy w zakresie dostępu do rejestru centralnego nie budziłoby wątpliwości, jeśli znajdowałoby odpowiednie umocowanie w przepisach – zarówno co do samego obowiązku prowadzenia badań i analiz, prawa dostępu do danych, jak i zakresu tego udostępniania. Pod rozwagę poddał kwestię, jaki zakres informacji o osobach fizycznych jest niezbędny do prowadzenia owych badań i analiz, w szczególności przez pryzmat kryterium niezbędności danych; nie można bowiem wykluczyć, że do ww. badań i analiz nie wystarczą jedynie dane statystyczne.

[197] Zasada legalizmu – art. 7 Konstytucji Rzeczypospolitej Polskiej, art. 6 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r. poz. 267).

Generalny Inspektor odniósł się ponadto do zagadnienia zgody na udział w badaniach rynku pracy – wyrażanej w związku z rejestracją w powiatowym urzędzie pracy[198]. O ile zatem obowiązujące przepisy stanowią o zgodzie osoby ubiegającej się o zarejestrowanie składanej wobec powiatowego urzędu pracy, o tyle w przedłożonej propozycji nie przewiduje się konstrukcji zgody na udział w takich badaniach, gdy administratorem danych jest minister właściwy do spraw pracy. Tym samym można przyjąć, że bez znaczenia jest zgoda ww. osoby wyrażona wobec powiatowego urzędu pracy, skoro minister właściwy do spraw pracy może w każdej sytuacji udostępnić dane tej osoby podmiotom prowadzącym badania i analizy rynku pracy na zlecenie publicznych służb zatrudnienia. Pod znakiem zapytania staje również możliwość realizacji podstawowych uprawnień osoby w zakresie zgody, w szczególności, możliwość odwołania zgody, skoro w ogóle nie istnieje oświadczenie woli osoby w tym zakresie. Ponadto obowiązujące przepisy nie przewidują wyrażania zgody na udział w badaniach rynku pracy przez osoby niezarejestrowane korzystające z pomocy określonej w ustawie oraz cudzoziemców zamierzających wykonywać lub wykonujących pracę na terytorium Rzeczypospolitej Polskiej, podczas gdy zakłada się przetwarzanie ich danych w rejestrach centralnych i udostępnianie z nich danych.

Zagadnienie udostępniania danych osobowych podmiotom prowadzącym badania i analizy rynku pracy zostało także poruszone wobec propozycji przepisów dotyczących rejestru bezrobotnych i poszukujących pracy prowadzonego przez powiatowe urzędy pracy, o którym to zagadnieniu będzie mowa w dalszej części *Sprawozdania*.

Kolejne przedstawiane Generalnemu Inspektorowi koncepcje uregulowania problematyki rejestrów centralnych nie były satysfakcjonujące. Brakowało w nich propozycji rozwiązań dających odpowiedzi na zasadnicze pytania dotyczące funkcjonowania rejestrów centralnych, pomimo iż wprowadzenie odpowiednich rozwiązań na poziomie ustawy zostało zadeklarowane na posiedzeniu stałego Komitetu Rady Ministrów w dniu 27 czerwca 2013 r. W trakcie pojawiły się też inne, generujące dodatkowe wątpliwości, rozwiązania. Na przykład zanegowana przez Generalnego Inspektora koncepcja gromadzenia w rejestrach centralnych również danych osób niezarejestrowanych, korzystających z pomocy określonej w ustawie

[198] § 5 ust. 12 rozporządzenia w sprawie rejestracji bezrobotnych i poszukujących pracy. Przepis ten stanowi bowiem, że osoba ubiegająca się o zarejestrowanie jako bezrobotny albo poszukujący pracy, może przekazać również numer telefonu i adres e-mail, celem ułatwienia kontaktu z urzędem pracy, oraz złożyć oświadczenie o wyrażeniu zgody na udział w badaniach rynku pracy prowadzonych przez publiczne służby zatrudnienia, organy administracji rządowej lub samorządowej lub na ich zlecenie.

(w trakcie prac legislacyjnych autorzy projektu zrezygnowali z tego rozwiązania). Koncepcje te dały podstawę do wnioskowania, że wolą projektodawcy było gromadzenie w przedmiotowym rejestrze centralnym szerokiego katalogu informacji o osobach fizycznych i jednocześnie skłoniła do postawienia pytania, czy w rejestrze centralnym – prowadzonym w innym celu niż rejestr bezrobotnych i poszukujących pracy – należy gromadzić wszystkie dane objęte rejestrem bezrobotnych i poszukujących pracy. Ilość danych przetwarzanych w tym drugim rejestrze jest przecież bardzo duża[199]. Trudno wyobrazić sobie uzasadnienie dla pozyskiwania i przetwarzania przez ministra właściwego do spraw pracy, danych zawartych w tychże dokumentach, np. w dokumentach potwierdzających stopień niepełnosprawności. Zakwestionowana przez Generalnego Inspektora została również prawidłowość odwoływania się do przepisów o narodowym zasobie archiwalnym i archiwach, jako źródła norm określających sposób postępowania z rejestrami centralnymi i zawartymi w nich danymi, w sytuacji, gdy przedmiotowe regulacje[200] dotyczyły m.in. takich kwestii, jak postępowanie z materiałami archiwalnymi i inną dokumentacją, działalność gospodarcza w zakresie przechowywania dokumentacji osobowej i płacowej pracodawców o czasowym okresie przechowywania, postępowanie z dokumentacją osobową i płacową w przypadku likwidacji lub upadłości pracodawcy. W efekcie nawarstwiających się wątpliwości autorzy projektu stwierdzili, iż kompleksowa regulacja tego kontrowersyjnego zagadnienia – które pierwotnie nie było objęte zakresem nowelizacji – mogłaby doprowadzić do opóźnień w pracach legislacyjnym nad – i tak już obszernymi – zmianami ustawy o promocji zatrudnienia i instytucjach rynku pracy. W związku z tym złożyli deklarację potwierdzoną przez Ministra Pracy i Polityki Społecznej, że zagadnienie to zostanie poruszone przy okazji kolejnej nowelizacji ww. ustawy, w której zapewniony zostanie udział Generalnego Inspektora Ochrony Danych Osobowych.

Poza tym Generalny Inspektor zgłosił także zastrzeżenia wobec rozwiązań prawnych zawartych w projektowanych przepisach dotyczących rejestrów lokalnych. Poruszył kwestię, czy rezygnacja z trybu wnioskowego udostępniania informacji z rejestru bezrobotnych i poszukujących pracy (aktualnie obowiązujący art. 33 ust. 8 ustawy o promocji zatrudnienia

[199] Powiatowym urzędom pracy, w związku z rejestracją bezrobotnych i poszukujących pracy, przysługuje uprawnienie np. do sporządzania kserokopii oraz skanów dokumentów (§5 ust. 5 rozporządzenia w sprawie rejestracji i bezrobotnych i poszukujących pracy).

[200] Zawarte w przepisach ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2011 r. Nr 123, poz. 698 z późn. zm.).

i instytucjach rynku pracy) i przyjęcie go jako ostatecznego trybu, właściwego do zastosowania jedynie w przypadku braku możliwości udostępnienia, pozyskania lub wymiany informacji (art. 33 ust. 8a projektu), nie wpłynie na zmniejszenie gwarancji ochrony danych osobowych (art. 33 ust. 7 projektu). Co więcej, jednocześnie poszerza się – i tak sformułowany w sposób niedookreślony – katalog podmiotów, którym dane z tego rejestru są udostępniane, włączając do niego *expressis verbis* podmioty prowadzące badania i analizy rynku pracy. Wyłania się dodatkowo pytanie, czy podmiotom tym – wobec braku sformułowanego w projektowanym przepisie ograniczenia co do zakresu udostępnianych danych – powinien zostać przyznany dostęp do wszystkich danych przetwarzanych w rejestrze bezrobotnych i poszukujących pracy, np. do danych o stanie zdrowia konkretnej osoby, oraz czy może właściwszym rozwiązaniem nie byłoby ustalenie pewnej restrykcji co do owego zakresu (np. do danych statystycznych).

Wobec przedłożenia przez projektodawcę w toku dalszych prac propozycji, aby udostępnianie informacji o bezrobotnych i poszukujących pracy ograniczone było przez kryterium „niezbędności dla realizacji zadań", Generalny Inspektor stwierdził, że aby mogło ono zostać uznane za wystarczające, z przepisów prawa wynikać powinien – w pierwszej kolejności – obowiązek wykonywania określonych zadań. Dopiero jeśli z przepisów wynikają określone obowiązki, to można rozważać konieczność dostępu do danych osobowych, która również powinna wynikać z powszechnie obowiązujących przepisów. Bez jednoznacznych, powszechnie obowiązujących norm w tym zakresie, niemożliwe jest przyjęcie, że podmiotom niepublicznym, a więc niezwiązanym zasadą legalizmu, przyznane zostanie uprawnienie do dostępu do danych osobowych szerokiego kręgu osób fizycznych, i to danych o rozległym zakresie, w tym obejmującym dane szczególnie chronione. Nasuwać się może wniosek wręcz przeciwny, tj. zakładający, że dla realizacji zadań oceny skuteczności udzielanej pomocy lub poprawy funkcjonowania publicznych służb zatrudnienia, wcale niekonieczne jest dysponowanie dostępem do danych osobowych, a wystarczyć mogą dane statystyczne. Ponadto w przypadku administratora danych, jakim są publiczne służby zatrudnienia, ustawodawca nie powinien dopuszczać do sytuacji, że o zakresie udostępniania na rzecz – określonych jedynie funkcjonalnie – podmiotów, administrator ten będzie każdorazowo rozstrzygał w umowie.

Odnosząc się do trybu udostępniania danych z rejestru bezrobotnych i poszukujących pracy, Generalny Inspektor podniósł rezygnację z trybu wnioskowego jako podstawowego

trybu udostępniania informacji, obowiązującego dotychczas przy udostępnianiu danych przez powiatowe urzędy pracy[201]. Wskazywał przyjęcie zamiast niego, w odniesieniu do udostępniania danych na poziomie zarówno województwa, jak i powiatu, dostępu online, oraz uczynienie trybu wnioskowego trybem awaryjnym wykorzystywanym w przypadku braku możliwości realizacji tego pierwszego trybu[202]. GIODO podkreślił, że w obowiązujących przepisach prawa dotyczących innych sektorów, udostępnianie w trybie online dopuszczane jest co do zasady na rzecz wąskiego katalogu służb i organów publicznych, powołanych do realizacji szczególnych zadań. Jako przykład wskazał na rozwiązanie dotyczące udostępniania Policji – w celu zapobiegania lub wykrywania przestępstw – danych telekomunikacyjnych przez podmiot prowadzących działalność telekomunikacyjną, jak również udostępniania danych telekomunikacyjnych na rzecz Straży Granicznej lub udostępniania danych lub informacji zgromadzonych w centralnej ewidencji pojazdów oraz z centralnej ewidencji kierowców. Jednocześnie Generalny Inspektor, jako nierozwikłane w materii projektu, uznał zagadnienie tego, w jaki sposób administrator danych, zezwalając na dostęp online, badałby, że dostęp do danych jest nadzorowany i rejestrowany zgodnie z przepisami o ochronie danych osobowych (czy podmioty, na rzecz których następuje udostępnienie, są zobowiązane do wykazywania, że warunek ten jest spełniany?)[203]. Zapytał również, na jakie konkretnie podmioty projektodawca nakłada obowiązek udostępniania danych. Z zaproponowanych przepisów nie wynikało jasno, jakie podmioty miałyby być zobligowane do udostępniania danych z wykorzystaniem systemów teleinformatycznych.

W toku prac legislacyjnych nad projektem ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy, na etapie prac w Komisji Prawniczej, projektodawcy wyeliminowali podmioty prowadzące badania i analizy rynku pracy z katalogu podmiotów, na rzecz których następuje udostępnienie danych osobowych. Przedstawiono koncepcję, zgodnie którą w przypadku służb zatrudnienia na poziomie województwa udostępnianie będzie następowało na rzecz publicznych służb zatrudnienia lub innych podmiotów realizujących zadania na podstawie ustawy lub odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny, w zakresie niezbędnym do prawidłowej realizacji tych zadań; w przypadku powiatowych urzędów pracy udostępnianie będzie

[201] Art. 33 ust. 7 ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[202] Projektowany art. 8 ust. 1d i ust. 1e oraz art. 33 ust. 8 i ust. 8a ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[203] Projektowany art. 8 ust. 1c pkt 3 i art. 33 ust. 8 ustawy o promocji zatrudnienia i instytucjach rynku pracy.

następowało na rzecz publicznych służb zatrudnienia lub innych podmiotów realizujących zadania na podstawie ustawy lub odrębnych przepisów, albo na skutek powierzenia lub zlecenia przez podmiot publiczny w zakresie niezbędnym do realizacji tych zadań, w szczególności jednostkom organizacyjnym pomocy społecznej oraz jednostkom obsługującym świadczenia rodzinne.

Natomiast w zakresie trybu udostępniania ostatecznie zaproponowano wprowadzenie alternatywne między dwoma sposobami udostępniania (bez przyznawania któremukolwiek z nich pierwszorzędnej roli), które ma odbywać się w trybie i na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, tj.: 1) na podstawie wniosku złożonego w szczególności w formie dokumentu elektronicznego lub 2) z wykorzystaniem systemów teleinformatycznych, jeżeli wojewódzki urząd pracy oraz podmiot, o którym mowa w ust. 1c, spełnia łącznie następujące warunki: 1) posiada możliwość identyfikacji osoby uzyskującej informacje w systemie oraz zakresu, daty i celu ich uzyskania; 2) posiada zabezpieczenia uniemożliwiające wykorzystanie informacji niezgodnie z celem ich uzyskania; 3) dostęp do danych osobowych jest nadzorowany i rejestrowany zgodnie z przepisami o ochronie danych osobowych.

Generalny Inspektor przedstawił również obszerne zastrzeżenia wobec zaproponowanej w projekcie założeń i rozwiniętej w projektowanych przepisach ustawy koncepcji profilowania osób bezrobotnych. GIODO zgodził się z projektodawcą, że profilowanie osób bezrobotnych może w wydatny sposób przyczynić się do poprawy działania systemu wsparcia w poszukiwaniu pracy. Takie działanie może znacząco poprawić również zarządzanie zasobami informacyjnymi dotyczącymi osób bezrobotnych oraz ofert pracy. W tej sytuacji tworzenie profili osobowych może zostać uznane za uzasadnione, a swoisty monopol służb wskazanych w ustawie w ustalaniu profilu pomocy może być wskazany. Tym nie mniej Generalny Inspektor wskazał, że twórcy reformy muszą zdawać sobie sprawę, że profilowanie jako takie prowadzi do naruszenia prywatności osoby. Proces profilowania prowadzone przez podmioty niedziałające na rynku konkurencyjnym prowadzi do wzrastającego zagrożenia dyskryminacją na podstawie danych "niezależnych" od woli osoby poddanej profilowaniu. W sytuacji, gdy - co podkreślił Minister Pracy i Polityki Społecznej - gestorzy baz centralnych nie nadzorują hierarchicznie działań starostów i urzędów pracy, pojawia się znaczące zagrożenie wymknięcia się systemu profilowania spod kontroli.

Twórcy projektu podczas posiedzenia Komitetu Rady Ministrów podkreślali, że profilowanie będzie miało ograniczony charakter i czynione będzie wyłącznie w celu pomocy osobom profilowanym. Nie negując dobrej woli twórców projektu Generalny Inspektor zauważył, że wyjaśnienia te są zbliżone do opinii rynku marketingu bezpośredniego, banków i ubezpieczycieli z pierwszej połowy lat 90-tych. Należy podejrzewać, że rozwój profilowania bezrobotnych będzie postępował podobną drogą, jak rozwój profilowania na tamtych rynkach. Wręcz zaskakujące byłoby, gdyby analitycy Ministerstwa Pracy i Polityki Społecznej oraz urzędów pracy nie wykorzystywali rozwiązań *business intelligence* dla profilowania bezrobotnych, jeśli narzędzia te są dostępne. Ta sytuacja - w związku z brzmieniem przepisów art. 31 i 51 Konstytucji Rzeczypospolitej Polskiej - powoduje, że sposób tworzenia profili, ich transmisji pomiędzy bazami, retencji i usuwania powinien być dokładnie opisany w ustawie. Z obecnego brzmienia projektu ustawy Generalny Inspektor nie jest w stanie wyprowadzić wiedzy o tych zagadnieniach.

Generalny Inspektor wyjaśnił, że profilowaniem nazywamy dwie grupy czynności podejmowanych przez przetwarzającego dane. W pierwszej zbierane są dane z różnych źródeł, o których wiadomo, że dotyczą tej samej zidentyfikowanej osoby. Jest to więc operacja obejmująca zespół technik *data miningu* dokonywana na zbiorach, w których przetwarzamy dane, co do których mamy silne podstawy by sądzić, że dotyczą one tej samej osoby i są one wystarczająco dobrej jakości, by wspólnie tworzyć wartość dodaną.

W drugim rozumieniu profilowanie odnoszone do pojedynczej osoby polega na wnioskowaniu o cechach nieznanych dla *data minera* z cech przypisanych już wcześniej danej osobie. Ta metoda obejmuje zazwyczaj tworzenie profilów grupowych, w których gromadzone są cechy wielu osób, umożliwiając statystyczne wnioskowanie o występowaniu cechy, której u danej osoby nie znamy, na podstawie przynależności tej osoby do populacji wykazującej te same cechy, które u danej osoby już rozpoznaliśmy.

Metoda uzupełniania zestawu cech osobowych o cechy, których występowania nie jesteśmy pewni, ale których możemy się na podstawie analizy danych statystycznych spodziewać, jest szczególnie niebezpieczna z punktu widzenia ochrony prywatności. O ile bowiem w pierwszym z opisanych przypadków mamy do czynienia z zestawianiem cech, które zdaniem przetwarzającego są prawdziwe dla danej osoby, o tyle w drugim przypadku nawet przetwarzający uznaje możliwość istnienia błędu w opisie osoby, ale uznaje – racjonalnie lub nie – że błąd taki może pominąć. Pierwsza z metod ingeruje więc przede

wszystkim w autonomię informacyjną osoby powodując, że dane na jej temat zestawiane są ponad standard jaki wynika z prawa i ponad zakres na jaki osoba się zgodziła. Druga z metod zaś prowadzi wprost do tworzenia profilów nieprawdziwych, przy których dla oceny przetwarzającego błąd nie jest znaczący. Takie postępowanie rodzi duże zagrożenie naruszenia podstawowych praw i wolności obywateli, a w szczególności rodzi niebezpieczeństwo dyskryminacji ze względu na płeć, pochodzenie etniczne i rasowe, wyznanie i przekonania, niepełnosprawność, wiek czy orientację seksualną, które zwiększane jest zakładaną przez przetwarzającego niedokładnością danych. Oba opisane wyżej procesy nie muszą być rozłączne, można nawet zaryzykować stwierdzenie, że drugi z procesów jest z reguły poprzedzany przez pierwszy, jako że wnioskowanie o danych statystycznie prawdziwych jest szczególnie przydatne w sytuacji, gdy danych pewnych jest wiele i gdy można na nich przeprowadzać wielorakie symulacje, co do przynależności osoby do grup wzorcowych.

Można z pewnym uproszczeniem przyjąć, że „profil" oznacza zestaw danych charakteryzujący kategorię osób, który ma zostać zastosowany odniesieniu do danej osoby. „Tworzeniem profili" określamy zaś automatyczną technikę przetwarzania danych polegającą na przypisaniu danej osobie „profilu" w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw. Wyjaśniając istotę problemu Generalny Inspektor powołał się na dwa różne podejścia do tworzenia profili użytkowników, wyróżniane przez Grupę Roboczą art. 29 zrzeszająca odpowiedników GIODO z wszystkich państw członkowskich Unii Europejskiej. A mianowicie profile predykcyjne, które tworzy się w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w określonym czasie (w szczególności poprzez monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które klika) oraz profile jawne tworzone na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez osoby, których dane dotyczą, np. podczas rejestracji. Wspomniane podejścia można łączyć. Ponadto profile predykcyjne mogą stać się jawne później, kiedy osoba, której dotyczą dane, utworzy dane logowania dla konkretnej strony internetowej. W odniesieniu do profilowania Generalny Inspektor wskazał także na wadliwość rozwiązania zakładającego pozbawienie osoby statusu bezrobotnego w przypadku niewyrażenia przez nią zgody na określenie profilu

pomocy[204]. W relacji organ administracji publicznej/obywatel trudno jest bowiem mówić o równości, która warunkuje z kolei dobrowolność zgody, będącą – stosownie do art. 2 lit. h dyrektywy nr 95/46/WE[205] – jej immanentną cechą. Ponadto skoro w przepisach projektu tworzy się określony model funkcjonowania publicznych służb zatrudnienia, którego obligatoryjnym i nieodłącznym elementem ma stać się proces profilowania, to obowiązek poddania się temu mechanizmowi także powinien wynikać z przepisów ustawy. Nie powinno się zaś wprowadzać koncepcji fikcyjnej zgody obejmującej fragment działań realizowanych przez urzędy pracy wobec obywateli.

Poruszając kwestię profilowania na etapie prac nad nowelizacją ustawy o promocji zatrudnienia i instytucjach rynku pracy w Sejmie Rzeczypospolitej Polskiej, Generalny Inspektor – wobec nieuwzględnienia jego postulatów zgłaszanych na wcześniejszych etapach – po raz kolejny krytycznie odniósł się do braku należytego uregulowania tego zagadnienia[206]. Podkreślił, że nie dysponuje wiedzą na temat metod skutecznej walki z bezrobociem i nie jest jego intencją kwestionowanie słuszności wprowadzania tego instrumentu służącego optymalizacji działań publicznych służb zatrudnienia. Jednak, aby istniała możliwość oceny profilowania pod kątem zgodności z przepisami o ochronie danych osobowych, konieczne jest jego pełne i kompleksowe, odpowiadające fundamentalnym wymogom wynikającym z Konstytucji Rzeczypospolitej Polskiej i ustawy o ochronie danych osobowych, uregulowanie tej materii w przepisach projektowanej ustawy. Zgodnie z propozycją przedstawioną przez projektodawcę, przy określaniu profilu mają być pod brane uwagę dwie zmienne: oddalenie od rynku pracy i gotowość do powrotu na rynek pracy[207]. O ile ta pierwsza zmienna wydaje się być możliwa do zdefiniowania przy użyciu przesłanek obiektywnych, o tyle druga z wymienionych jawi się jako mało obiektywna, a wręcz umożliwiająca podejmowanie przez urzędnika publicznych służb zatrudnienia subiektywnych decyzji. Co więcej, na podstawie tych zmiennych mają być przygotowywane indywidualne plany działania, a tym samym niewykluczone jest, że raz przyporządkowany do klienta urzędu pracy profil, może za nim „podążać" w dalszym ciągu korzystania z usług publicznych

[204] Projektowany art. 33 ust. 4 pkt 1a ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[205] Dyrektywa nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, str. 31 z późn. zm.).
[206] Projektowany art. 9 ust. 1 pkt 4a, art. 33 ust. 2a i ust. 4 pkt 1a, art. 34a ust. 1, 3 i 3c ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[207] Projektowany art. 33 ust. 2a ustawy o promocji zatrudnienia i instytucjach rynku pracy.

służb zatrudnienia. Wątpliwości tej nie wyeliminowała norma przewidująca możliwość modyfikacji indywidualnego planu działania stosownie do zmieniającej się sytuacji bezrobotnego i poszukującego pracy[208], ponieważ nie nakłada w tym zakresie żadnych obowiązków ani nie precyzuje, na podstawie jakich kryteriów owa modyfikacja miałaby być dokonywana. Powyższe daje podstawy do wnioskowania, że działania podejmowane przez urzędy pracy mogą być w istocie niczym innym, jak profilowaniem predykcyjnym. Tymczasem z projektu niemożliwa do wyprowadzenia była wiedza na temat tak zasadniczych aspektów profilowania, jak elementy, które się na profilowanie składają, zasady jego tworzenia, okres przechowywania danych przetwarzanych w związku z profilowaniem, czy będą niszczone, czy przekazywane dalej, itd. Generalny Inspektor stwierdził, że dostrzega w projekcie przepis stanowiący o delegacji dla ministra właściwego do spraw pracy do określenia w drodze rozporządzenia, trybu ustalania profilu pomocy oraz sposobu postępowania w ramach określonego profilu[209], oraz przepis, który upoważnia do uregulowania w drodze aktu wykonawczego szczegółowych warunków realizacji, trybu i sposobów prowadzenia przez urzędy pracy usług rynku pracy[210]. Niemniej jednak, podkreślić trzeba, że akt podustawowy – rozporządzenie lub stosowane przez publiczne służby zatrudnienia kwestionariusze – nie może stanowić źródła norm prawnych określających zakres danych przetwarzanych w procesie profilowania lub okresu ich przechowywania. Z ustawy powinno być możliwe – tak dla organu do spraw ochrony danych osobowych, jak i milionów obywateli korzystających z usług publicznych służb zatrudnienia – pozyskanie wiedzy o zasadniczych elementach składających się na ten instrument wsparcia w walce z bezrobociem, które to stwierdzenie wydaje się zyskać poparcie w orzeczeniu Europejskiego Trybunału Praw Człowieka w sprawie *Amman przeciwko Szwajcarii* z dnia 16 lutego 2000 r.

Prace nad projektem ustawy o promocji zatrudnienia i instytucjach rynku pracy trwały również w roku 2014 r. przy aktywnym uczestnictwie Generalnego Inspektora Ochrony Danych Osobowych, który kontynuował przedstawianie uwag dotyczących profilowania osób bezrobotnych zarówno w formie pism kierowanych do podkomisji stałej do spraw rynku

[208] Projektowany art. 34a ust. 3a ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[209] Projektowany art. 34a ust. 3c ustawy o promocji zatrudnienia i instytucjach rynku pracy.
[210] Projektowany art. 35 ust. 5 ustawy o promocji zatrudnienia i instytucjach rynku pracy.

pracy, Komisji Polityki Społecznej i Rodziny, jak i osobistego uczestnictwa w posiedzeniach ww. komisji Sejmu Rzeczypospolitej Polskiej[211].

Kolejnym istotnym projektem opiniowanym przez Generalnego Inspektora było **rozporządzenie Ministra Pracy i Polityki Społecznej zmieniające rozporządzenie w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego[212]**, który jednak nie został bezpośrednio skierowany do zaopiniowania GIODO. A ponieważ dotyczył centralnego rejestru osób bezrobotnych i poszukujących pracy, w związku z czym uwagi przedstawione przez organ do spraw ochrony danych osobowych nawiązywały do polemiki wyrażonej w odniesieniu do projektu założeń projektu ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy.

W pierwszej kolejności Generalny Inspektor poddał w wątpliwość przepis, zgodnie z którym marszałek województwa sprawdza za pomocą rejestru centralnego osób bezrobotnych i poszukujących pracy, o którym mowa w art. 4 ust. 4 ustawy i zwanego dalej „rejestrem centralnym", informacje o bezrobotnym, dotyczące w szczególności okresów uprawniających go do zasiłku oraz posiadania statusu osoby bezrobotnej[213]. Wskazał, że ustawa o promocji zatrudnienia i instytucjach rynku pracy w żadnym ze swych przepisów nie wskazuje szczegółowego zakresu danych zawartych w owym rejestrze. Stanowi jedynie, że rejestr ten zawiera m.in. dane dotyczące poszukujących pracy i bezrobotnych gromadzone przez publiczne służby zatrudnienia na podstawie przepisów ustawy, i że jest on zasilany danymi przekazywanymi przez te służby[214]. Sformułowanej w ten sposób normie GIODO zarzucił, że nie daje odpowiedzi na pytanie, jakie dane dotyczące bezrobotnego podlegają weryfikacji przez marszałka województwa. Tym samym z przepisu odnoszącego się do jednego z elementów procedury ustalania prawa do zasiłku, osoby fizyczne ubiegające się o zasiłek nie będą w stanie wysnuć wniosku co do zakresu informacji, które będą sprawdzane w procedurze prowadzącej do rozstrzygnięcia o przyznaniu lub odmowie przyznania im tego uprawnienia. Skoro przepisy prawa określają, jakie kryteria leżą u podstaw podjęcia rozstrzygnięcia, o którym mowa w rozporządzeniu Ministra Pracy i Polityki Społecznej

[211] Ustawa z dnia 14 marca 2014 r. o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw została ogłoszona w Dz. U. 2014 poz. 598.
[212] DOLiS-033-153/13
[213] § 1 pkt 1 projektu dotyczący dodawanego ust. 1a w § 2 rozporządzeniu Ministra Pracy i Polityki Społecznej z dnia 18 sierpnia 2009 r. w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego (Dz. U. Nr 136, poz. 1118 oraz z 2010 r. Nr 173, poz. 1174).
[214] – art. 4 ust. 4 i ust. 5 *in principio* ustawy o promocji zatrudnienia i instytucjach rynku pracy.

w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego[215], należałoby w przepisach wskazać także, co miałoby podlegać sprawdzeniu za pomocą rejestru centralnego. Treść ww. przepisu powinna zostać doprecyzowana o wskazanie elementów, jakie marszałek województwa ma obowiązek zweryfikować przed wydaniem decyzji o przyznaniu albo odmowie przyznania prawa do zasiłku dla bezrobotnych.

Analogiczną uwagę Generalny Inspektor sformułował w odniesieniu do przepisu, który nie określał, jakie dokładnie informacje uzyskane z rejestru centralnego stanowią podstawę przyznania prawa do zasiłku dla bezrobotnych, a wskazywał jedynie, że są to informacje „dotyczące w szczególności rejestracji bezrobotnego"[216]. Generalny Inspektor wskazał zatem na konieczność uściślenia, co składa się na owe niezbędne informacje, tak aby również osoby będące zainteresowane rozstrzygnięciem w przedmiocie przyznania im zasiłku dla bezrobotnych miały świadomość, jakie dane ich dotyczące podlegają przetwarzaniu w procesie podejmowania tego rozstrzygnięcia z wykorzystaniem rejestru centralnego.

W odpowiedzi na kolejną wersję projektu[217], Generalny Inspektor podtrzymał zastrzeżenia dotyczące braku precyzji przepisu, w którym mowa o wydawaniu rozstrzygnięcia w przedmiocie przyznania albo odmowy przyznania osobie fizycznej zasiłku dla bezrobotnych na podstawie danych uzyskanych z rejestru centralnego[218]. Nadal bowiem nie wynikało z niego, jakie dane dotyczące bezrobotnego podlegają weryfikacji przez marszałka województwa. Sformułowanie „niezbędne dane" nie wskazuje, jakie dane osobowe będą podstawą podejmowania rozstrzygnięcia w przedmiocie przyznania albo odmowy przyznania osobie fizycznej zasiłku dla bezrobotnych. Wskazał ponadto, że przepis ten – w celu ustalenia zbioru informacji wykorzystywanych do wydania określonego rozstrzygnięcia - dotyczy

[215] § 2 ust. 1 rozporządzeniu Ministra Pracy i Polityki Społecznej z dnia 18 sierpnia 2009 r. w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego.
[216] § 1 pkt 2 projektu – w zakresie dotyczącym treści § 2 ust. 2 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 18 sierpnia 2009 r. w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego.
[217] W wersji oznaczonej jako „Projekt z dnia 13 maja 2013 r."
[218] § 1 pkt 1 projektu, dotyczący § 2 ust. 4 rozporządzenia z dnia 18 sierpnia 2009 r. w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego. Zgodnie z projektem tego przepisu wydanie rozstrzygnięcia, o którym mowa w ust. 1, następuje na podstawie (….) niezbędnych danych, o których mowa w przepisach wykonawczych wydanych na podstawie art. 33 ust. 5 ustawy, uzyskanych z rejestru centralnego udostępnionego przez ministra właściwego do spraw pracy, zwanego dalej „rejestrem centralnym".

rozporządzenia w sprawie rejestracji bezrobotnych i poszukujących pracy[219], które reguluje zakres danych o bezrobotnych, ale zgromadzonych w rejestrze bezrobotnych i poszukujących pracy prowadzonym przez powiatowe urzędy pracy. Natomiast w dalszej części komentowanego przepisu znajduje się stwierdzenie, że dane określone w tymże rozporządzeniu mają być uzyskiwane z rejestru centralnego udostępnianego przez ministra właściwego do spraw pracy. Rozporządzenie w sprawie rejestracji bezrobotnych i poszukujących pracy – warto podkreślić – nie odnosi się do zakresu danych zawartych w rejestrze centralnym, bowiem zgodnie z wolą ustawodawcy do jego materii przekazane zostało uregulowanie szeregu kwestii związanych z innym rejestrem, tj. rejestrem bezrobotnych i poszukujących pracy. Do rejestrów centralnych odnosi się jednak zupełnie inny przepis niż wskazany w proponowanej treści przepisu rozporządzenia. Generalny Inspektor – analogicznie jak w uwagach do projektu założeń projektu ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz projektu ww. ustawy – podkreślił, że przepisy ustawy o promocji zatrudnienia i instytucjach pracy nie wskazują precyzyjnie merytorycznego zakresu informacji zawartych w rejestrach centralnych prowadzonych przez ministra właściwego do spraw pracy. Nierozstrzygnięta pozostaje kwestia, jakimi danymi owe rejestry centralne są zasilane, bowiem powołany przepis tego nie precyzuje. Nie wydaje się więc uprawnione, aby z takiego stwierdzenia w przepisach można było wyprowadzać wniosek, że rejestr centralny zawierający „(…) dane dotyczące poszukujących pracy, bezrobotnych (…) gromadzone przez publiczne służby zatrudnienia na podstawie przepisów ustawy[220]”, jest tożsamy z rejestrem bezrobotnych i poszukujących pracy w zakresie gromadzonych tam informacji. Jeśli zatem podstawę do wydania rozstrzygnięcia, o którym mowa w rozporządzeniu w sprawie szczegółowego trybu przyznawania zasiłku dla bezrobotnych, stypendium i dodatku aktywizacyjnego, mają stanowić dane pozyskane z określonego zbioru danych, to należy stworzyć przepis, który po pierwsze, jednoznacznie wskaże te **dane**, a po drugie wskaże przedmiotowy **zbiór danych** w sposób właściwy. Co więcej, sam zbiór powinien być na tyle uregulowany w przepisach, że nie pozostawi wątpliwości, jakie dane będą ewentualnie brane pod uwagę przy podejmowaniu rozstrzygnięcia. W aktualnym stanie prawnym stwierdzenie o pozyskiwaniu danych z rejestru

[219] Rozporządzenie z dnia 12 listopada 2012 r. w sprawie rejestracji bezrobotnych i poszukujących pracy (Dz. U. z 2012 r. poz. 1299).
[220] Art. 4 ust. 4 ustawy o promocji zatrudnienia i instytucjach rynku pracy.

centralnego nie wydaje się być trafione, skoro nieuregulowane w przepisach pozostają tak istotne z punktu widzenia jego funkcjonowania kwestie, jak zakres gromadzonych w nim danych, cel jego stworzenia, czy też zasady prowadzenia rejestru przez ministra właściwego do spraw pracy. W dalszej korespondencji dotyczącej projektu Generalny Inspektor powołał się na dyskusję i wymianę pism między Generalnym Inspektorem Ochrony Danych Osobowych a Ministrem Pracy przy okazji prac legislacyjnych nad projektem **założeń projektu ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw.**

Generalny Inspektor w okresie sprawozdawczym ustosunkował się ponadto do projektu **ustawy o Bankowym Funduszu Gwarancyjnym, uporządkowanej likwidacji banków oraz o zmianie niektórych innych ustaw[221].** Opiniując przedmiotowy projekt autorstwa resortu finansów zgłosił zastrzeżenia m.in. do propozycji normy, która przewidywała udostępnianie Funduszowi danych dotyczących klientów ujętych w systemach wyliczania (tj. systemach informatycznych podmiotów objętych systemem gwarantowania, przeznaczonym do zapewnienia możliwości niezwłocznego uzyskania wszelkich danych pozwalających na identyfikację deponentów oraz określenie wysokości należnych poszczególnych deponentom środków gwarantowanych[222]), zawartych w zbiorach prowadzonych przez podmioty lub osoby trzecie, w szczególności dane ze zbiorów meldunkowych, zbioru danych osobowych PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych, o których mowa w odrębnych przepisach[223]. Nie wynikało z niej bowiem, na jakich konkretnie podmiotach/organach spoczywa obowiązek udostępnienia Bankowemu Funduszowi Gwarancyjnemu danych z prowadzonych przez nie zbiorów. Wiadomo jedynie, że skuteczne żądanie może zostać skierowane do organów, o których w obecnym stanie prawnym stanowi ustawa o ewidencji ludności i dowodach osobistych[224]. Skoro pewne podmioty mają zostać obarczone obowiązkiem udostępnienia określonych danych z administrowanych przez siebie zbiorów danych, to należy stworzyć przepis, który jednoznacznie wskaże katalog podmiotów, których ten obowiązek dotyczy. Nie powinno się przyjmować rozwiązania, które jedynie przykładowo wymienia podmioty zobowiązane do takiego działania, pomijając inne

[221] DOLiS-033-188/13
[222] Definicja zawarta w art. 2 pkt 21 projektu.
[223] Art. 30 ust. 3 projektu.
[224] Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych, Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.

i stwarzając jednocześnie możliwość rozszerzającej interpretacji w zakresie kręgu podmiotów zobligowanych do działania związanego z przetwarzaniem danych osobowych. Innymi słowy, jeśli Bankowy Fundusz Gwarancyjny ma dysponować uprawnieniem do żądania dostępu do określonych zbiorów i znany jest cel przyznania tego uprawnienia – kontrola prawidłowości danych zawartych w systemie wyliczania – to konstruowane rozwiązanie nie powinno budzić wątpliwości w kwestii tego, do kogo to żądanie może być skutecznie kierowane.

Zastrzeżenia Generalnego Inspektora wzbudziła ponadto propozycja, zgodnie z którą „zarząd Funduszu ustala zasady i tryb stwierdzania tożsamości deponenta w trakcie wypłat (…)"[225]. Projektodawca zdecydował, że zasady i tryb stwierdzania tożsamości nie będą określone w tym akcie prawnym, lecz w innym dokumencie, i to najprawdopodobniej – skoro ma on być ustalany przez zarząd funduszu – o charakterze wewnętrznym. Ustalone mają w nim zostać dane identyfikujące deponenta, których umieszczenie na liście wypłat jest niezbędne do ustalenia tożsamości deponenta[226] przez podmiot dokonujący wypłat, mając na uwadze powszechność posługiwania się tymi danymi przez deponentów oraz możliwość dokonania za pomocą tych danych jednoznacznej identyfikacji deponenta[227], czy rodzaje dokumentów stwierdzających tożsamość, za pomocą których podmiot dokonujący wypłat będzie identyfikował deponentów ubiegających się o wypłatę świadczeń gwarantowanych[228]. Generalny Inspektor stwierdził, że jeśli nie istnieją szczególne przeszkody, owe zasady i tryb można by, chociaż ogólnie, wskazać w niniejszym projekcie. Jeśli zaś przedmiotem takiej regulacji miałyby być bardziej kwestie techniczne niż zasadnicze, możliwe do zaakceptowania byłoby również określenie zasad i trybu w drodze rozporządzenia, co należałoby ewentualnie stwierdzić w treści projektowanego przepisu ustawy. Obecnie sformułowana propozycja, nie wskazując sposobu uregulowania ww. zagadnień, sugeruje, że będą one określone w dokumencie wewnętrznym nienależącym do katalogu źródeł powszechnie obowiązującego prawa Rzeczypospolitej Polskiej. Tym samym projekt „wymyka się" w tym zakresie merytorycznej ocenie organu do spraw ochrony danych osobowych.

Organ do spraw ochrony danych osobowych wskazał także na potrzebę doprecyzowania przepisu dotyczącego treści wniosku do Komisji Nadzoru Finansowego o wydanie

[225] Art. 44 projektu
[226] Zgodnie z art. 2 pkt 5 projektu deponentem może być również osoba fizyczna.
[227] Art. 44 pkt 1 projektu
[228] Art. 44 pkt 2 projektu

zezwolenia na utworzenie banku pomostowego poprzez określenie, jakie konkretnie dane dotyczące osób przewidzianych do objęcia w banku pomostowym stanowisk członków zarządu należy tam zamieścić[229]. Doprecyzowanie treści tego przepisu jest zalecane tym bardziej, że w projekcie przewiduje się jednocześnie dokonywanie przez Komisję Nadzoru Finansowego kontroli w zakresie zupełności wniosku i przyznanie jej uprawnienia do wezwania do jego uzupełnienia[230]. Przez wzgląd na zasadę adekwatności przetwarzanych danych organ do spraw ochrony danych osobowych wskazał również na potrzebę doprecyzowania projektowanego przepisu ustawy - Kodeks postępowania cywilnego[231], poprzez wskazanie zakresu informacji zawartych w „wykazie wierzycieli banku w likwidacji", która jest załączana do wniosku o wszczęcie postępowania.

W okresie sprawozdawczym Generalny Inspektor uczestniczył również w opiniowaniu rządowego projektu **ustawy o zasadach prowadzenia zbiórek publicznych[232]**, wobec którego zgłosił szereg uwag, jak również uczestniczył w spotkaniach jego dotyczących. Zastrzeżenia zgłoszone zostały m.in. do propozycji przepisu, który przewidując, że w akcie założycielskim zawarte są w szczególności „dane osoby upoważnionej do reprezentowania komitetu społecznego", nie wskazuje jednak, jakie konkretne miałyby być to dane[233]. Analogiczną uwagę sformułował wobec propozycji normy, w której mowa była o „danych osoby upoważnionej do reprezentowania organizatora zbiórki"[234].

W wątpliwość poddana również została norma nakładają na osoby tworzące komitet założycielski, obowiązek załączenia do formularza zgłoszenia zbiórki publicznej oświadczeń wszystkich członków komitetu społecznego o niekaralności za popełnienie określonych w jego treści przestępstw lub wykroczeń, pod rygorem odpowiedzialności karnej[235]. Powstało bowiem pytanie, dlaczego projektodawca zdecydował się na badanie karalności – za pomocą oświadczeń – osób tworzących komitet społeczny organizujący zbiórkę publiczną, a nie wprowadził już takiego badania w stosunku do osób będących członkami pozostałych podmiotów, o których mowa w art. 3 projektu. Wobec przedstawionych w trakcie spotkania

[229] Art. 121 ust. 1 pkt 2 lit a projektu.
[230] Art. 121 ust. 4. Projektu.
[231] Art. 216 projektu, w zakresie dotyczącym zmian art. 694^{18} § 2 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.).
[232] DOLiS-033-210/13
[233] Art. 4 ust. 2 pkt 3 projektu
[234] Art. 7 ust. 1 pkt 2 projektu
[235] Art. 10 pkt 2 projektu

roboczego wyjaśnień, z których wynikało, iż jest to jedyna metoda sprawdzania wiarygodności osób fizycznych tworzących komitet założycielski, pozostawienie tego rozwiązania w projekcie zostało uznane za uzasadnione.

W trakcie prac legislacyjnych dodany został przepis przewidujący, że organizator zbiórki zapewnia identyfikatory osobom przeprowadzającym zbiórkę publiczną, zawierające w szczególności informacje o nazwie i celu zbiórki publicznej, jej organizatorze oraz imię i nazwisko osoby zbierającej. Rozumiejąc ewentualną potrzebę, aby na identyfikatorze zawarte były pewne dodatkowe informacje związane ze zbiórką publiczną, których celem byłoby zapewnienie większej transparentności, Generalny Inspektor stwierdził, że takie sformułowanie przepisu umożliwia zawarcie na przedmiotowym identyfikatorze dowolnych danych osobowych osób przeprowadzających zbiórkę. Działanie takie mogłoby natomiast spotkać się z zarzutem naruszenia - omawianej w ramach ww. opinii organu do spraw ochrony danych osobowych wobec projektu - zasady adekwatności danych w stosunku do celu ich przetwarzania. Aby zatem wyeliminować możliwość dowolnej interpretacji treści komentowanej normy i ryzyka zamieszczania na identyfikatorze danych w zakresie szerszym niż konieczny do realizacji celu przepisu (tj. zapewnienia informacji o zbiórce publicznej i osób ją przeprowadzających) Generalny Inspektor zasugerował zmianę jej treści w taki sposób, który ograniczy zakres danych osobowych uwidoczniony na identyfikatorze, a jednocześnie umożliwi zawarcie dodatkowych informacji dotyczących samej zbiórki, który to postulat został przez projektodawców zrealizowany.

Generalny Inspektor krytycznie odniósł się do propozycji przewidującej udostępnianie zgłoszeń zbiórki publicznej wraz ze sprawozdaniami, o których mowa w art. 15, na portalu zbiórek publicznych przez okres co najmniej 5 lat od dnia ich zamieszczenia[236]. Stwierdził, że rozwiązanie takie pozostaje w sprzeczności z dyspozycją art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych, który to przepis nakłada na administratorów danych obowiązek zapewnienia, by przetwarzane przez nich dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania. W związku z powyższym, nie negując zasadności zapewnienia powszechnej dostępności informacji dotyczących zbiórek publicznych, w tym weryfikowania ich za pośrednictwem ww. portalu przez opinię publiczną w określonej

[236] Art. 18 projektu

perspektywie czasowej, organ do spraw ochrony danych osobowych wskazał na konieczność poprawienia dyspozycji powołanego przepisu poprzez wskazanie w nim precyzyjnie okresu, przez który informacje te będą dostępne na portalu zbiórek publicznych, np. poprzez usunięcie z komentowanego przepisu sformułowania „co najmniej". Bez dodatkowego uzasadnienia w tym zakresie wątpliwość wzbudziło również ustanowienie w treści ww. przepisu obowiązku tak długiego okresu udostępniania zgłoszeń zbiórek publicznych wraz ze sprawozdaniami, na portalu zbiórek publicznych. Kwestia okresu zamieszczania na portalu zbiórek publicznych zgłoszeń zbiórki publicznej była podnoszona również w toku dalszych prac nad projektem. W stanowisku skierowanym do Sejmowej Komisji Administracji i Cyfryzacji, wobec zawarcia w projekcie przepisu ustanawiającego jedynie dolną granicę okresu zamieszczania danych osobowych na ww. portalu, Generalny Inspektor podkreślił, że taka norma umożliwi *de facto* nieograniczone w czasie przechowywanie danych, naruszając tym samym zasadę ograniczenia czasowego[237]. Na dalszym etapie prac w Sejmie Rzeczypospolitej Polskiej, wobec przyjęcia rozwiązania zakładającego 10-letni okres zamieszczania zgłoszeń zbiórek publicznych na portalu, GIODO skonstatował, że propozycja ta kierunkowo jest właściwa – ustanawia bowiem konkretny czas przechowywania informacji, w tym danych osobowych. Pod rozwagę Komisji poddał natomiast kwestię, czy rzeczywiście dla zapewnienia zbiórkom publicznym transparentności i kontroli społecznej, niezbędne jest udostępnianie ww. informacji przez tak długi, 10-letni, okres. Poprzednia propozycja nominalnie odnosiła się do okresu 3 lat, stąd tak istotne wydłużenie – mimo iż wykluczające możliwość dłuższego niż wskazany w treści przepisu czas – skłoniło do postawienia pytania o uzasadnienie dla wyznaczenia takiego horyzontu czasowego, który bezwzględnie wydaje się okresem długim. Prace w Sejmie nad projektem zakończyły się jednak pozostawieniem rozwiązania przewidującego 10-letni okres zamieszczania zgłoszenia zbiórki na portalu zbiórek publicznych[238].

W okresie sprawozdawczym 2013 roku Generalny Inspektor zajął również stanowisko wobec rządowego projektu **ustawy o zmianie ustawy – Prawo o ustroju sądów**

[237] Art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych.
[238] Ustawa z dnia 14 marca 2014 r. o zasadach prowadzenia zbiórek publicznych opublikowana została w Dz. U. 2014 poz. 498.

powszechnych, ustawy o Krajowej Radzie Sądownictwa oraz o zmianie niektórych innych ustaw[239].

W projekcie tym wątpliwości GIODO wzbudziła propozycja, zgodnie z którą do karty zgłoszenia dołącza się również oświadczenie w przedmiocie zgody na wykorzystanie dokumentów dotyczących zgłaszającego w innych postępowaniach w sprawie powołania do pełnienia urzędu na stanowisku sędziowskim[240]. Z tak sformułowanego przepisu wynikało bowiem, że na kandydatów na wolne stanowiska sędziowskie nakłada się obowiązek wyrażenia zgody na przetwarzanie danych osobowych na potrzeby kolejnych postępowań w sprawie powołania do pełnienia urzędu na stanowisku sędziowskim. Abstrahując od praktyki występującej po stronie kandydatów na wolne stanowiska sędziowskie, która świadczyć może o powszechności zainteresowania takim przetwarzaniem w związku z przyszłymi postępowaniami, stwierdzić jednak należy, że niewłaściwe jest rozwiązanie, które zgodę taką wymusza na podstawie przepisu prawa, odbierając tym samym owemu oświadczeniu woli walor dobrowolności. Właściwszą konstrukcją byłoby ustanowienie w projektowanym przepisie prawnej możliwości dołączenia do zgłoszenia przedmiotowego oświadczenia. Innymi słowy, oświadczenie to powinno być dołączane jedynie fakultatywnie, przez osoby zainteresowane takim wykorzystaniem dokumentów w ramach innych postępowań w sprawie powołania do pełnienia urzędu na stanowisku sędziowskim.

GIODO zgłosił ponadto uwagę dotyczącą składania przez kandydata oświadczeń, włącznie z oświadczeniem, że nie toczy się wobec niego inne postępowanie w sprawie powołania do pełnienia urzędu na stanowisku sędziowskim[241]. Powyższą konstrukcję można by przyjąć bez zastrzeżeń jedynie w sytuacji, w której kandydat zawsze będzie posiadał wiedzę o toczących się wobec niego postępowaniach. Tymczasem, możliwa wydaje się okoliczność, że osoba, której dane dotyczą, składając oświadczenie o zgodzie na wykorzystanie dokumentów jej dotyczących w innych postępowania w sprawie powołania do pełnienia urzędu na stanowisku sędziowskim, może nie dysponować informacjami w tym zakresie i mimo braku złej woli, złożyć nieprawdziwe oświadczenie, narażając się na odpowiedzialność karną. W związku z powyższym rozważenia wymaga, czy przepis ten powinien obejmować swym zakresem także powołane wyżej oświadczenie.

[239] DOLiS-033-479/13
[240] Art. 1 pkt 7 projektu, w zakresie dotyczącym art. 57 §7 zdanie drugie ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, Dz. U. z 2013 r. poz. 427 i 662.
[241] Projektowany art. 57 §8 ustawy – Prawo o ustroju sądów powszechnych.

Przystępując do opiniowania poselskiego projektu **ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw**[242] (druk sejmowy nr 946), który to projekt nie został przesłany do organu do spraw ochrony danych osobowych pomimo, iż dotyczył kwestii przetwarzania danych osobowych, Generalny Inspektor Ochrony Danych Osobowych w pierwszej kolejności zakwestionował art. 20 i ust. 2 i art. 20 j ust. 4 ustawy z dnia 10 kwietnia 1997 roku – Prawo energetyczne (t. j. Dz. U. z 2006 r. Nr 89, poz. 625 z późn. zm.)[243]. W obu przepisach w sposób wadliwy określony został zakres danych, jakie mogą być przetwarzane na ich podstawie. W pierwszym z nich wyliczenie danych osobowych zostało bowiem poprzedzone formułą „w szczególności", w drugim zaś – „co najmniej". Tym samym katalog danych osobowych, do których przetwarzania przepisy te uprawniają, zyskał charakter otwarty. Rozwiązanie takie pozostaje zaś w sprzeczności z wiążącą administratorów danych zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane[244].

Za wadliwe GIODO uznał także, użyte w art. 20 i ust. 2 pkt 3 ustawy – Prawo energetyczne, sformułowanie, w myśl którego wniosek o wydanie certyfikatu instalatora mikroinstalacji lub małej instalacji zawiera: „numer PESEL albo rodzaj i numer innego dokumentu potwierdzającego tożsamość[245]. Identyczna uwaga do wyżej zamieszczonej została również zgłoszona do art. 20 za ust. 2 pkt 3 ustawy – Prawo energetyczne[246]. Generalny Inspektor Ochrony Danych Osobowych stwierdził potrzebę doprecyzowania art. 20 q ust. 3 pkt 6 ustawy – Prawo energetyczne. Przy zaproponowanym w projekcie ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw brzmieniu tego przepisu nie można byłoby bowiem stwierdzić, jakie konkretnie dane osób prowadzących zajęcia teoretyczne i praktyczne mają znaleźć się w – przygotowywanym przez podmiot ubiegający się o uzyskanie akredytacji Prezesa Urzędu Dozoru Technicznego – wykazie osób.

[242] DOLiS-033-5/13

[243] Dodawane przez art. 1 pkt 14 projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw.

[244] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

[245] Zgodnie z art. 31 a ust. 1 ustawy z dnia 10 kwietnia 1974 roku o ewidencji ludności i dowodach osobistych (t.j. Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.) – numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (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 – liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego", nie zaś dokument.

[246] Dodawanego przez art. 1 pkt 14 projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw.

Możliwość zaś zamieszczenia w wykazie dowolnych danych osób prowadzących zajęcia teoretyczne i praktyczne narusza zasadę adekwatności przetwarzanych danych w stosunku do celów ich przetwarzania[247]. Porównanie treści art. 20 i ust. 2 ustawy – Prawo energetyczne, regulującego zakres informacji zawartych we wniosku o wydanie certyfikatu instalatora mikroinstalacji lub małej instalacji z art. 20 za ust. 2 ustawy – Prawo energetyczne[248], określającym katalog informacji zamieszczanych w – prowadzonym przez Prezesa Urzędu Dozoru Technicznego – rejestrze certyfikowanych instalatorów, wydanych certyfikatów i ich wtórników, zrodziło po stronie GIODO pytanie o źródło informacji, z którego Prezes Urzędu Dozoru Technicznego pozyskać ma, mającą być zamieszczaną w rejestrze certyfikowanych instalatorów, wydanych certyfikatów i ich wtórników, daną o miejscu urodzenia instalatora. Wniosek o wydanie certyfikatu instalatora mikroinstalacji lub małej instalacji danej takiej bowiem nie zawiera. Podkreślić przy tym trzeba, iż brak ten nie może być uzupełniony z wykorzystaniem, użytej w art. 20 i ust. 2 ustawy – Prawo energetyczne, formuły „w szczególności".

W związku z deklarowaną w art. 20 za ust. 6 ustawy – Prawo energetyczne zasadą jawności rejestru akredytowanych organizatorów szkoleń, organ do spraw ochrony danych osobowych zauważył potrzebę dostosowania tego przepisu do unormowań zawartych w ustawie z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej (t. j. Dz. U. z 2010 r. Nr 220, poz. 1447 z późn. zm.), odnoszących się do zakresu jawności danych osób fizycznych prowadzących działalność gospodarczą. Skoro – zgodnie z art. 20 za ust. 5 ustawy – Prawo energetyczne w zw. z art. 20 q ust. 2 pkt 1 tejże ustawy, w jawnym rejestrze akredytowanych organizatorów szkoleń ma być zamieszczany adres organizatora szkoleń, to – analogicznie jak ma to miejsce w art. 37 ust. 1 pkt 1 ustawy o swobodzie działalności gospodarczej – w art. 20 za ust. 6 ustawy – Prawo energetyczne powinien być przewidziany wyjątek od zasady jawności rejestru akredytowanych organizatorów szkoleń, w myśl którego nie jest ujawniany (upubliczniany) adres osoby fizycznej organizującej szkolenia jeżeli jest inny, aniżeli adres miejsca prowadzenia przez nią tej działalności. Generalny Inspektor Ochrony Danych Osobowych konsekwentnie stoi na stanowisku, że adres osoby fizycznej prowadzącej określoną działalność tylko wówczas może być uznany za informację (daną)

[247] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.
[248] Dodawanego przez art. 1 pkt 14 projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw.

identyfikującą tę osobę w obrocie i – w konsekwencji – upubliczniany, gdy jest tożsamy z miejscem prowadzenia przez tę osobę tej działalności. W wypadku zaś, gdy adres osoby fizycznej prowadzącej określoną działalność jest inny, aniżeli adres miejsca prowadzenia przez tę osobę działalności, dana ta podlega ochronie na podstawie przepisów ustawy o ochronie danych osobowych i nie powinna być upubliczniana.

W toku dalszych prac legislacyjnych prowadzonych w podkomisji nadzwyczajnej do rozpatrzenia poselskiego projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (druk nr 946) Ministerstwo Gospodarki zgłosiło do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw poprawkę[249] mającą na celu unormowanie kwestii tzw. „liczników inteligentnych"[250]. Generalny Inspektor Ochrony Danych Osobowych zaoponował przeciwko takiemu rozwiązaniu stwierdzając, że wprowadzenie systemów inteligentnego pomiaru energii, choć może przyczynić się do zracjonalizowania zużycia energii przez odbiorców i pozytywnie wpłynąć na wysokość płaconych przez nich rachunków, będzie miało jednocześnie istotny wpływ na prawo do prywatności i ochrony danych osobowych odbiorców energii. Dlatego też zagadnienie tzw. „liczników inteligentnych", będące przedmiotem szczególnego zainteresowania organu do spraw ochrony danych osobowych, nie powinno być wprowadzane w drodze poprawki do poselskiego projektu ustawy dotyczącego innych kwestii i bez przeprowadzenia stosownych konsultacji[251].

Wobec podtrzymania przez Ministerstwo Gospodarki jego propozycji, GIODO skierował do podkomisji nadzwyczajnej do rozpatrzenia poselskiego projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (druk nr 946) kolejne pismo[252], w którym skrytykował projektowane uregulowania odnoszące się do tzw. „inteligentnych liczników". Według Generalnego Inspektora Ochrony Danych Osobowych zaprezentowane w dokumencie „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946)" brzmienie art. 9 u i art. 9 w ustawy – Prawo energetyczne oznacza, iż zamiarem Ministerstwa Gospodarki było wprowadzenie innego modelu systemu inteligentnego pomiaru energii, aniżeli proponowany wcześniej

[249] Dokument „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946)".
[250] Zagadnienie to nie było objęte pierwotnym przedłożeniem zawartym w druku sejmowym nr 946.
[251] Pismo z dnia 23 stycznia 2013 roku o sygn. DOLiS-033-5/13/TG/4233.
[252] DOLiS-033-5/13/13977, 13980.

w projektowanej nowej ustawie – Prawo energetyczne (stanowiącej jeden z elementów tzw. „Trójpaku Energetycznego"). O ile bowiem w ramach prac legislacyjnych dotyczących wspomnianego „Trójpaku Energetycznego" Ministerstwo Gospodarki opowiadało się za modelem, w którym dane pomiarowe zebrane przez tzw. „inteligentne liczniki" miały być przekazywane niezwłocznie przez operatorów systemów elektroenergetycznych do centralnego zbioru informacji pomiarowych prowadzonego przez Zarządcę Rozliczeń S.A., zaś podmiot ten miał udostępniać odpłatnie jednostkowe dane pomiarowe dotyczące danego odbiorcy końcowego operatorowi systemu dystrybucyjnego elektroenergetycznego, do którego sieci są przyłączone urządzenia, instalacje lub sieci odbiorcy końcowego, to w modelu zaproponowanym w dokumencie „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946)" operator systemu dystrybucyjnego elektroenergetycznego (OSD) zobowiązany do przekazywania do centralnego zbioru informacji pomiarowych danych pomiarowych zebranych przez liczniki zdalnego odczytu (art. 9 u ust. 2 ustawy – Prawo energetyczne) może jednocześnie przechowywać te dane pomiarowe we własnym zbiorze danych i wykorzystywać na własne potrzeby (art. 9 u ust. 3 ustawy – Prawo energetyczne). Takie rozwiązanie rodziło pytania po co tworzyć centralny zbiór danych zawierający informacje stanowiące w istocie sumę informacji już zgromadzonych w zbiorach danych będących w posiadaniu operatorów systemów elektroenergetycznych oraz w jakim celu dane zawarte w centralnym zbiorze danych mają być zindywidualizowane, czyli pozwalać na identyfikację konkretnego odbiorcy końcowego? Ponadto pojawiały się istotne pytania o zasady przetwarzania danych zgromadzonych w zbiorach danych prowadzonych przez operatorów systemu dystrybucyjnego elektroenergetycznego.

Zbiory danych pomiarowych prowadzone przez operatorów systemu dystrybucyjnego elektroenergetycznego stanowią zbiory danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych. Tymczasem, odmiennie aniżeli ma to miejsce w odniesieniu do centralnego zbioru informacji pomiarowych prowadzonego przez Zarządcę Rozliczeń S.A., dla którego to zbioru przewidziano wydanie przez ministra właściwego do spraw gospodarki rozporządzenia regulującego sposób przetwarzania i przechowywania informacji

pomiarowych[253], w przypadku zbiorów danych pomiarowych prowadzonych przez operatorów systemu dystrybucyjnego elektroenergetycznego brak jest propozycji unormowań dotyczących zasad przetwarzania danych w tych zbiorach. Dodatkowo nie może umknąć uwadze, iż operator systemu dystrybucyjnego elektroenergetycznego sam decydowałby o celach przetwarzania danych pomiarowych przez siebie zebranych[254], co nie może spotkać się z aprobatą ze strony organu do spraw ochrony danych osobowych.

Powyższe ustalenia dotyczące modelu systemu inteligentnego pomiaru energii doprowadziły GIODO do stwierdzenia, że rozwiązanie zaproponowane w art. 9 w ust. 3 pkt 2 lit. b ustawy – Prawo energetyczne[255] jest nielogiczne i merytorycznie nieprawidłowe. Skoro bowiem w myśl art. 9 u ust. 3 ustawy – Prawo energetyczne operator systemu dystrybucyjnego elektroenergetycznego może gromadzić na własne potrzeby bez żadnych ograniczeń dane pomiarowe we własnym zbiorze danych, to nie wydaje się możliwe, by był zainteresowany zakupem od operatora informacji pomiarowych (Zarządcy Rozliczeń S.A.) jednostkowych danych pomiarowych w zakresie danych archiwalnych dotyczących odbiorcy końcowego, którego urządzenia, instalacje lub sieci są bezpośrednio przyłączone do jego sieci, gdyż może takie dane posiadać od chwili ich pozyskania z liczników zdalnego odczytu bez ponoszenia dodatkowych kosztów. Co więcej – w art. 9 w ust. 3 pkt 2 lit. b ustawy – Prawo energetyczne nie wprowadzono definicji pojęcia „dane archiwalne”**.** Za niezrozumiałe i nieakceptowalne Generalny Inspektora Ochrony Danych Osobowych uznał także unormowanie z art. 9 w ust. 3 pkt 1 lit. b ustawy – Prawo energetyczne, zgodnie z którym operator informacji pomiarowych miałby udostępniać jednostkowe (czyli umożliwiające identyfikację konkretnego odbiorcy końcowego) dane pomiarowe ministrowi właściwemu do spraw gospodarki narodowej na potrzeby prowadzenia badań statystycznych z zakresu rynku paliwowo-energetycznego**.** Organ do spraw ochrony danych osobowych nie znalazł argumentów, które przemawiałyby za przekazywaniem ministrowi właściwemu do spraw gospodarki narodowej zindywidualizowanych danych będących danymi osobowymi dla

[253] Art. 9 z ust. 1 pkt 7 ustawy – Prawo energetyczne w brzmieniu nadanym w dokumencie „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946)”.
[254] Art. 9 u ust. 3 ustawy – Prawo energetyczne w brzmieniu nadanym w dokumencie „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946); użyte w komentowanym przepisie pojęcie „własnych potrzeb” operatora systemu elektroenergetycznego nie zostało w tym dokumencie w żaden sposób sprecyzowane.
[255] W brzmieniu nadanym w dokumencie „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946)”.

celów analitycznych i statystyczno – sprawozdawczych**.** W ocenie GIODO ponownej analizy wymagało również brzmienie projektowanych art. 9 g ust. 1 a oraz art. 9 z ust. 1 ustawy – Prawo energetyczne, gdyż dyspozycje tych przepisów w pewnej części pokrywały się. Na przykład zarówno w instrukcji postępowania z informacjami pomiarowymi, jak i w rozporządzeniu określającym szczegółowe zasady funkcjonowania systemu opomiarowania, miałyby być uregulowane kwestie zakresu informacji pomiarowych oraz bezpieczeństwa informacji pomiarowych. W ocenie organu do spraw ochrony danych osobowych pierwszeństwo powinno zostać przyznane rozporządzeniu określającemu szczegółowe zasady funkcjonowania systemu opomiarowania jako aktowi prawnemu powszechnie obowiązującemu. To w przedmiotowym rozporządzeniu winny się zatem znaleźć regulacje odnoszące się do zakresu informacji pomiarowych, częstotliwości ich zbierania, sposobu przetwarzania, okresu przechowywania i zapewnienia im bezpieczeństwa. Instrukcja postępowania z informacjami pomiarowymi, jako dokument wydany przez operatora informacji pomiarowych, może zaś zawierać jedynie normy techniczne i uszczegóławiające.

Wobec krytyki, również ze strony GIODO, rozwiązań zawartych w dokumencie „POPRAWKA do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Druk nr 946)" Podkomisja nadzwyczajna do rozpatrzenia poselskiego projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (druk nr 946) przyjęła na posiedzeniu w dniu 14 maja 2013 roku rozwiązania kompromisowe, które jednak nie zyskały akceptacji organu do spraw ochrony danych osobowych. W opinii GIODO[256], w następstwie usunięcia z projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw niektórych unormowań zamieszczonych w dokumencie „Sprawozdanie podkomisji nadzwyczajnej" (wersja z dnia 05.03.2013 r.), zaproponowane w dokumencie „Sprawozdanie podkomisji nadzwyczajnej" (wersja z dnia 14.05.2013 r.) brzmienie art. 9 c ust. 5 a i 5 b ustawy – Prawo energetyczne[257] nie może zostać zaakceptowane przez organ do spraw ochrony danych osobowych. Regulacje te – mające w zamierzeniu autorów iść naprzeciw postulatom Generalnego Inspektora Ochrony Danych Osobowych co do zapewnienia w projekcie ustawy o zmianie ustawy – Prawo energetyczne

[256] Pismo z dnia 22 maja 2013 roku o sygn. DOLiS-033-5/13/TG/31872.
[257] Dodawanym przez art. 1 pkt 12 lit. d projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw.

oraz niektórych innych ustaw ochrony praw odbiorców energii elektrycznej wynikających z przepisów ustawy o ochronie danych osobowych – sprawiają bowiem wrażenie niejako „wyrwanych z kontekstu". Projektowany art. 9 c ust. 5 a ustawy – Prawo energetyczne[258] nakłada na operatorów systemów dystrybucyjnych instalujących u odbiorców końcowych liczniki zdalnego odczytu, obowiązek chronienia – na zasadach określonych w ustawie o ochronie danych osobowych – danych pomiarowych dotyczących tych odbiorców. Tymczasem zarówno w oparciu o przepisy projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw, jak i unormowania obowiązującej ustawy – Prawo energetyczne, nie można w sposób jednoznaczny ustalić znaczenia terminu „dane pomiarowe". Z uwagi na fakt, że definicja pojęcia „dane pomiarowe"[259] „wypadła" z projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw, powstaje zasadnicza wątpliwość, co w istocie chronić mają operatorzy systemów dystrybucyjnych.

Zasadniczo wadliwa jest również definicja terminu „liczniki zdalnego odczytu", gdyż dotknięta jest ona błędem nazywanym *ignotum per ignotum*[260]. Skoro bowiem – w myśl projektowanego art. 9 c ust. 5 b ustawy – Prawo energetyczne – przez „liczniki zdalnego odczytu rozumie się zespół urządzeń służących do pozyskiwania danych pomiarowych, umożliwiający dwustronną komunikację z systemem teleinformatycznym", to „definicja" taka niczego nie wyjaśnia. Obok istotnych wątpliwości w kwestii znaczenia terminu „dane pomiarowe", przyjęta przez podkomisję nadzwyczajną do rozpatrzenia poselskiego projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (druk nr 946), wersja projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw[261] nie zawiera przepisów, które pozwalałyby stwierdzić, między jakimi podmiotami miałaby się odbywać „dwustronna komunikacja", o której mowa w projektowanym art. 9 c ust. 5 b ustawy – Prawo energetyczne i jakie informacje (dane) miałyby być w ramach tej dwustronnej komunikacji przekazywane. Co więcej – w przepisach projektu ustawy o zmianie

[258] Dodawany przez art. 1 pkt 12 lit. d projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw, w brzmieniu nadanym temu projektowi w dokumencie „Sprawozdanie podkomisji nadzwyczajnej" (wersja z dnia 14.05.2013 r.).

[259] Zamieszczona poprzednio w art. 3 pkt 50 ustawy – Prawo energetyczne, dodawanym przez art. 1 pkt 1 lit. h *projektu ustawy o zmianie ustawy* – Prawo energetyczne oraz niektórych innych ustaw, w brzmieniu nadanym temu projektowi w dokumencie „Sprawozdanie podkomisji nadzwyczajnej" (wersja z dnia 05.03.2013 r.)

[260] *Ignotum per ignotum* - łac. „nieznane przez nieznane" – błąd logiczny popełniany podczas definiowania, który polega na zbyt skomplikowanym wyjaśnianiu definiowanego terminu.

[261] Dokument „Sprawozdanie podkomisji nadzwyczajnej" (wersja z dnia 14.05.2013 r.).

ustawy – Prawo energetyczne oraz niektórych innych ustaw nie wskazano także, o jaki system teleinformatyczny w projektowanym art. 9 c ust. 5 b ustawy – Prawo energetyczne, chodzi.

Uwagi Generalnego Inspektora Ochrony Danych Osobowych zostały zignorowane przez Parlament, który przyjął ustawę z dnia 26 lipca 2013 roku o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Dz. U. z 2013 r. poz. 984) zawierającą zakwestionowane wyżej unormowania.

Opiniując projekt **ustawy o systemie powiadamiania ratunkowego**[262] GIODO stwierdził potrzebę doprecyzowania dyspozycji art. 9 ust. 2 pkt 2 tego projektu, który to przepis upoważnia do przetwarzania w systemie teleinformatycznym służącym do wykonywania zadań centrum powiadamiania ratunkowego oraz współpracujących systemach teleinformatycznych Policji, Państwowej Straży Pożarnej, dyspozytorów medycznych i innych podmiotów, do których zadań należy ochrona życia, zdrowia, bezpieczeństwa ludności, a także mienia i środowiska, danych osobowych zgłaszającego oraz ustalonych uczestników zdarzenia, bez wskazania, o jakie dane chodzi. Uwzględniając, że pojęcie „dane osobowe" obejmuje swoim zakresem wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[263], przyjęcie kwestionowanego unormowania w proponowanym brzmieniu prowadziłoby do sytuacji, w której w – wyżej wymienionych – systemach teleinformatycznych mogłyby się znaleźć dowolne dane osób zgłaszających zdarzenia oraz uczestniczących w tych zdarzeniach. Takie sformułowanie przepisu pozostaje w sprzeczności z zasadą adekwatności przetwarzanych danych do celów, w jakich są przetwarzane[264]. W ocenie organu do spraw ochrony danych osobowych zachodziła zatem potrzeba zmiany brzmienia art. 9 ust. 2 pkt 2 projektu ustawy o systemie powiadamiania ratunkowego i jednoznacznego uregulowania w tym przepisie, jakie dane osób zgłaszających zdarzenia oraz uczestniczących w tych zdarzeniach mogą być przetwarzane w systemach teleinformatycznych w związku z przyjmowaniem zgłoszeń alarmowych. Tym bardziej, że pojęcie „dane osobowe zgłaszającego" występuje także w innych przepisach tego projektu (art. 7 ust. 1 pkt 3, art. 8 ust. 5).

GIODO zwrócił się także do projektodawcy o wyjaśnienie znaczenia, użytego w art. 8 ust. 5 *in fine* analizowanego aktu prawa, pojęcia „uprawniony organ", który może złożyć do

[262] DOLiS-033-54/13
[263] Art. 6 ust. 1 ustawy o ochronie danych osobowych.
[264] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

wojewody wniosek o udostępnienie danych zarejestrowanych w systemie teleinformatycznym służącym do wykonywania zadań centrum powiadamiania ratunkowego. Z treści projektu ustawy o systemie powiadamiania ratunkowego nie wynikało bowiem, jaki podmiot winien być uznany za „uprawniony organ" w rozumieniu art. 8 ust. 5 projektu, a tym samym – jaki podmiot (podmioty?) może uzyskać dostęp do danych osobowych zgromadzonych w systemie teleinformatycznym.

W toku dalszych prac legislacyjnych wskazane wyżej kwestie zostały wyjaśnione organowi do spraw ochrony danych osobowych, jednakże w projekcie ustawy o systemie powiadamiania ratunkowego znalazły się kolejne unormowania, które wzbudziły zastrzeżenia GIODO. I tak organ do spraw ochrony danych osobowych stwierdził[265], iż w art. 8 pkt 6 projektu ustawy o systemie powiadamiania ratunkowego[266] projektodawca zdecydował się na wydłużenie do 3 lat okresu przechowywania przez centrum powiadamiania ratunkowego danych dotyczących treści połączeń alarmowych[267]. W opinii Generalnego Inspektora Ochrony Danych Osobowych rozwiązanie takie było nieuzasadnione i pozostawało w sprzeczności z panującą tendencją do skracania okresu przechowywania danych umożliwiających identyfikację osób korzystających z systemów telekomunikacyjnych[268]. W ocenie organu do spraw ochrony danych osobowych dla realizacji celów wskazanych w uzasadnieniu projektu ustawy o systemie powiadamiania ratunkowego wystarczający jest jednoroczny okres przechowywania danych dotyczących treści połączeń alarmowych przewidziany we wcześniejszej wersji tego projektu[269]. Rozumiejąc przesłanki, które legły u podstaw propozycji zamieszczonej w art. 11 projektu ustawy o systemie powiadamiania ratunkowego, GIODO uznał przepis ten za zupełnie niezrozumiały w aktualnym brzmieniu. W oparciu o jego treść nie sposób ustalić, administratorem jakich danych jest minister właściwy do spraw administracji publicznej[270], nie wynika to bowiem z jego zdania

[265] Pismo z dnia 29 kwietnia 2013 roku o sygn. DOLiS-033-54/13/TG/26688.
[266] Wbrew stanowczemu sprzeciwowi wyrażonemu na konferencji uzgodnieniowej przez przedstawiciela GIODO.
[267] W tym nagrań zgłoszeń alarmowych skierowanych do danego centrum powiadamiania ratunkowego.
[268] W tej kwestii przykładowo wskazać należy zmianę 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. dokonaną przez art. 1 pkt 128 lit. a ustawy z dnia 16 listopada 2012 roku o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw – Dz. U. z 2012 r. poz. 1445.
[269] Wersja z dnia 25.01.2013 r.
[270] Minister Administracji i Cyfryzacji – §1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 roku w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji – Dz. U. Nr 248, poz. 1479

pierwszego. Z drugiej zaś strony sposób ujęcia zdania drugiego tego artykułu jest na tyle ogólny, że teoretycznie przepis ten umożliwiałby, w przypadku wejścia w życie, upoważnienie wszystkich osób do przetwarzania wszelkich danych, co nie może być zaakceptowane w świetle zasad ochrony danych osobowych określonych w ustawie o ochronie danych osobowych. Zastrzeżenia GIODO wzbudziła też propozycja zawarta w art. 8 ust. 1 pkt 5 projektu ustawy o systemie powiadamiania ratunkowego[271], bowiem przepis ten zobowiązując centrum powiadamiania ratunkowego do wymiany informacji i danych z Policją, Państwową Strażą Pożarną, dysponentami zespołów ratownictwa medycznego oraz podmiotami, których numery telefoniczne są obsługiwane w ramach systemu, nie wskazując przy tym, jakie informacje i dane mają być wymieniane. Projektodawca ograniczył się jedynie do enigmatycznego wskazania celu takiej wymiany, tj. „potrzeby analiz". Takie ujęcie kwestionowanego przepisu jest nieprecyzyjne i niespójne z rozwiązaniem przyjętym w art. 8 ust. 1 pkt 1 lit. e projektu ustawy o systemie powiadamiania ratunkowego, które wskazuje zakres wymiany danych o zgłoszeniach alarmowych przetwarzanych w systemie teleinformatycznym z określonymi w jego treści organami (Policją, Państwową Strażą Pożarną, dysponentami zespołów ratownictwa medycznego lub innymi podmiotami, których numery są obsługiwane w ramach systemu), stanowiąc o „zakresie określonym na podstawie art. 5 ust. 6 pkt 5 oraz art. 13 ust. 3 pkt 3".

Ostatecznie uwagi Generalnego Inspektora Ochrony Danych Osobowych zgłoszone wobec art. 8 ust. 1 pkt 5 oraz art. 11 projektu ustawy o systemie powiadamiania ratunkowego zostały uwzględnione. Jednakże w uchwalonej przez Parlament i podpisanej przez Prezydenta Rzeczypospolitej Polskiej ustawie z dnia 22 listopada 2013 roku o systemie powiadamiania ratunkowego (Dz. U. z 2013 r. poz. 1635) pozostał trzyletni okres przechowywania przez centrum powiadamiania ratunkowego w systemie teleinformatycznym, danych dotyczących treści połączeń alarmowych.

Do projektu **rozporządzenia Ministra Zdrowia w sprawie utworzenia Rejestru Medycznie Wspomaganej Prokreacji**[272] organ do spraw ochrony danych osobowych zgłosił dwie uwagi.

Po pierwsze, za nieprawidłowe uznał brzmienie § 2 ust. 3 pkt 2 tego projektu. Skoro – zgodnie z § 3 projektowanego aktu prawa – Rejestr Medycznie Wspomaganej Prokreacji

[271] Pismo z dnia 14 listopada 2013 roku o sygn. DOLiS-033-54/13/MK/75554.
[272] DOLiS-033-169/13

zawierać będzie dane szczególnie chronione w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, to sformułowanie § 2 ust. 3 pkt 2 projektu ww. rozporządzenia, które zezwalało na dowolną wymianę (a więc również przekazywanie innym podmiotom) danych zgromadzonych w tym rejestrze, musiało być uznane przez GIODO za niedopuszczalne. Dlatego organ do spraw ochrony danych osobowych wniósł o doprecyzowanie § 2 ust. 3 pkt 2 projektu rozporządzenia Ministra Zdrowia w sprawie utworzenia Rejestru Medycznie Wspomaganej Prokreacji poprzez wskazanie podmiotów (albo kategorii podmiotów), które będą uprawnione do udziału w wymianie danych (w tym danych szczególnie chronionych) zamieszczonych w tym Rejestrze. Po drugie, poprawienia wymagał § 3 pkt 3 lit. c projektu, gdyż przepis ten uprawniał do gromadzenia w Rejestrze Medycznie Wspomaganej Prokreacji „innego identyfikatora" dotyczącego usługobiorcy, nie precyzując wszakże, o jaki identyfikator chodzi.

Odnotować należy, iż wyżej wskazane uwagi Generalnego Inspektora Ochrony Danych Osobowych do projektu rozporządzenia Ministra Zdrowia w sprawie utworzenia Rejestru Medycznie Wspomaganej Prokreacji zostały w całości uwzględnione[273], co nie jest normą w przypadku aktów prawnych opracowywanych przez Ministerstwo Zdrowia.

Opiniując projekt **ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw**[274] (druk sejmowy nr 1278) GIODO stwierdził, że przewidziane w tym projekcie brzmienie nowego art. 132 a ustawy z dnia 11 września 2003 roku o służbie wojskowej żołnierzy zawodowych (t. j. Dz. U. z 2010 r. Nr 90, poz. 593 z późn. zm.)[275] było (w zakresie ustępu 5 tego artykułu) nie do zaakceptowania z punktu widzenia zasad ochrony danych osobowych. Powołany przepis[276] stanowi, że do przetwarzania przez organy wojskowe danych osobowych żołnierza pełniącego służbę kandydacką (w art. 48 ust. 6 ustawy o służbie wojskowej żołnierzy zawodowych – żołnierza zawodowego) nie stosuje się przepisów rozdziału 3 ustawy o ochronie danych osobowych. Takie brzmienie projektowanego art. 132 a ust. 5 ustawy o służbie wojskowej żołnierzy zawodowych (a także obowiązującego art. 48 ust. 6 ustawy o służbie wojskowej żołnierzy

[273] Rozporządzenie Ministra Zdrowia z dnia 14 czerwca 2013 roku w sprawie Rejestru Medycznie Wspomaganej Prokreacji – Dz. U. z 2013 r. poz. 721.
[274] DOLiS-033-177/13
[275] Dodawanego przez art. 1 pkt 63 projektu ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw.
[276] Podobnie jak niezmieniany w projekcie ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw art. 48 ust. 6 ustawy o służbie wojskowej żołnierzy zawodowych.

zawodowych) nie tylko pozostaje w sprzeczności z elementarnymi regułami odnoszącymi się do ochrony danych osobowych, lecz jest również nielogiczne. Wypada bowiem przypomnieć, iż rozdział 3 ustawy o ochronie danych osobowych zawiera unormowania dotyczące podstawowych zasad przetwarzania danych osobowych, a co za tym idzie – obowiązywanie regulacji z tego rozdziału *de facto* warunkuje stosowanie pozostałych przepisów ustawy o ochronie danych osobowych[277]. Tym samym wprowadzenie w projektowanym art. 132 a ust. 5 ustawy o służbie wojskowej żołnierzy zawodowych (w połączeniu z już obowiązującym art. 48 ust. 6 tejże ustawy) wyłączenia stosowania przepisów rozdziału 3 ustawy o ochronie danych osobowych, oznacza w rzeczywistości całkowite wyłączenie stosowania przepisów ustawy o ochronie danych osobowych w odniesieniu do - przetwarzanych w ewidencji wojskowej - danych osobowych żołnierzy pełniących służbę kandydacką i żołnierzy zawodowych.

Wyłączenie to nie daje się pogodzić z przepisami prawa polskiego oraz unormowaniami dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[278]. Dyrektywa ta przewiduje bowiem możliwość ograniczenia – w określonych sytuacjach – stosowania jej postanowień w pewnym zakresie, nie zezwala wszakże na całkowite wyłączenie stosowania jej unormowań. Co więcej, zgodnie z art. 28 ust. 1 przywołanej dyrektywy 95/46/WE, każde państwo członkowskie ma zapewnić, że jeden lub więcej organów władzy publicznej będzie odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów przyjętych na mocy tej dyrektywy. Skoro brzmienie projektowanego art. 132 a ust. 5 ustawy o służbie wojskowej żołnierzy zawodowych (w powiązaniu z obowiązującym art. 48 ust. 6 ustawy o służbie wojskowej żołnierzy zawodowych) faktycznie niweczy możliwość sprawowania przez Generalnego Inspektora Ochrony Danych Osobowych kontroli prawidłowości z punktu widzenia ochrony danych osobowych przetwarzania w ewidencji wojskowej danych żołnierzy pełniących służbę kandydacką i żołnierzy zawodowych, niezgodność projektowanego art. 132 a ust. 5 ustawy o służbie wojskowej żołnierzy zawodowych i obowiązującego art. 48 ust. 6 tejże ustawy z – wiążącymi Rzeczypospolitą Polską – przepisami prawa europejskiego GIODO uznał za

[277] Dotyczących choćby kompetencji Generalnego Inspektora Ochrony Danych Osobowych – art. 12 pkt 1, 2 i 4 ustawy o ochronie danych osobowych.
[278] Dz. Urz. WE L 281 z 23.11.1995, str. 31 z późn. zm.

bezsporną. Dlatego też organ do spraw ochrony danych osobowych wniósł o zmianę propozycji brzmienia nowego art. 132 a ustawy o służbie wojskowej żołnierzy zawodowych[279] poprzez usunięcie z tego przepisu jednostki redakcyjnej oznaczonej jako ustęp 5 oraz o uzupełnienie projektu ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw o przepis uchylający art. 48 ust. 6 ustawy o służbie wojskowej żołnierzy zawodowych.

Uwagi GIODO do ww. projektu spotkały się z akceptacją podkomisji nadzwyczajnej do rozpatrzenia rządowego projektu ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw (druk nr 1278), która wniosła poprawki do przedłożenia rządowego. Zgodnie ze zgłoszonymi poprawkami, w art. 48 ust. 6 ustawy o służbie wojskowej żołnierzy zawodowych[280] i w art. 132 a ust. 5 ustawy o służbie wojskowej żołnierzy zawodowych[281] zawarto sformułowanie: „Przetwarzanie danych osobowych […] zgromadzonych w ewidencji wojskowej może odbywać się bez wiedzy i zgody osoby, której dotyczą te dane". W ocenie Generalnego Inspektora Ochrony Danych Osobowych takie ujęcie powyższych przepisów zapewni zgodność ustawy o służbie wojskowej żołnierzy zawodowych z zasadami ochrony danych osobowych określonymi w ustawie o ochronie danych osobowych i uwzględni jednocześnie specyficzne potrzeby Wojska Polskiego w zakresie pozyskiwania informacji o żołnierzach zawodowych[282].

Opiniując projekt **rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego**[283], który to projekt nie został przesłany do organu do spraw ochrony danych osobowych pomimo, iż dotyczył bezpośrednio problematyki ochrony danych osobowych, GIODO podniósł, iż w istniejącym stanie prawnym brak jest podstawy ustawowej dla prowadzenia monitoringu pokojów izolacyjnych, które mają być tworzone w strzeżonych ośrodkach dla cudzoziemców[284]. Nie można zaś zaakceptować, by proponowany § 3 ust. 4

[279] Zamieszczonej w art. 1 pkt 63 projektu ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw.
[280] Art. 1 pkt 31 projektu ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw.
[281] Art. 1 pkt 63 projektu ustawy o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz o zmianie niektórych innych ustaw.
[282] Ustawa o zmianie ustawy o służbie wojskowej żołnierzy zawodowych oraz niektórych innych ustaw została uchwalona na 51. posiedzeniu Sejmu Rzeczypospolitej Polskiej w dniu 11 października 2013 roku – Dz. U. z 2013 r. poz. 1355 (korekty tytułu ustawy dokonano w czasie prac w Parlamencie).
[283] DOLiS-033-197/13
[284] Biorąc pod uwagę, że – zgodnie z rozdziałem 9 i 10 ustawy z dnia 13 czerwca 2003 roku o cudzoziemcach - t. j. Dz. U. z 2011 r. Nr 264, poz. 1573 z późn. zm. – strzeżone ośrodki dla cudzoziemców nie są miejscami

projektowanego rozporządzenia, stanowił jedyną podstawę prawną dla monitorowania pokojów izolacyjnych w strzeżonych ośrodkach dla cudzoziemców, gdyż monitorowanie pomieszczenia, w którym – przymusowo[285] – przebywa cudzoziemiec, stanowi wkroczenie w sferę jego gwarantowanego konstytucyjnie[286] prawa do prywatności. Zgodnie zaś z art. 31 ust. 3 zdanie pierwsze Konstytucji Rzeczypospolitej Polskiej 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. Tak więc, o ile samo zastosowanie wobec cudzoziemca środka przymusu bezpośredniego w postaci pokoju izolacyjnego, w razie zaistnienia którejś z przesłanek wymienionych w art. 11 pkt 3, 4, 6, 8 i 14 projektowanej ustawy o środkach przymusu bezpośredniego i broni palnej, stanowić będzie dozwolone ograniczenie jego konstytucyjnych praw[287], to dla wprowadzenia całodobowego monitorowania pokojów izolacyjnych niezbędne jest zamieszczenie stosownych regulacji w ustawie o cudzoziemcach (normującej zasady prowadzenia strzeżonych ośrodków i umieszczania w nich cudzoziemców) albo projektowanej ustawie o środkach przymusu bezpośredniego i broni palnej (określającej zasady stosowania środka przymusu bezpośredniego w postaci pokoju izolacyjnego). Wobec braku takich unormowań w wymienionych ustawach propozycja zawarta w §3 ust. 4 projektu rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego wykracza poza zakres wyznaczony przez podustawowy, wykonawczy charakter aktu prawnego, jakim jest rozporządzenie[288]. Wobec powyższego organ do spraw ochrony danych osobowych wniósł o usunięcie z projektu rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego, § 3 ust. 4 oraz – w konsekwencji – również § 4 pkt 2 lit. c tegoż projektu.

Generalny Inspektor Ochrony Danych Osobowych zakwestionował także sposób wykonania przez Ministra Spraw Wewnętrznych w projektowanym rozporządzeniu delegacji ustawowej z art. 29 ust. 3 pkt 2 projektowanej ustawy o środkach przymusu bezpośredniego i broni palnej. W przepisie tym ustawodawca nałożył na ministra właściwego do spraw

---

publicznie dostępnymi, przepisem rangi ustawowej upoważniającym do wprowadzenia monitoringu w takich ośrodkach nie może być art. 11 ust. 1 pkt 7 ustawy z dnia 12 października 1990 roku o Straży Granicznej - t. j. Dz. U. z 2011 r. Nr 116, poz. 675, z późn. zm.

[285] Art. 29 ust. 1 projektowanej ustawy o środkach przymusu bezpośredniego i broni palnej.

[286] Art. 47 w zw. z art. 37 ust. 1 Konstytucji Rzeczypospolitej Polskiej.

[287] Jeśli ten środek przymusu bezpośredniego będzie wykonywany prawidłowo.

[288] Art. 92 ust. 1 zdanie pierwsze Konstytucji Rzeczypospolitej Polskiej.

wewnętrznych[289] obowiązek określenia, w drodze rozporządzenia, okresu przechowywania, sposobu archiwizowania lub brakowania dokumentacji dotyczącej osób umieszczonych w pokoju izolacyjnym, a także formy tej dokumentacji. Tymczasem w projekcie rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego poprzestano na uregulowaniu (§7 projektu) formy dokumentacji dotyczącej umieszczenia cudzoziemca w pokoju izolacyjnym (notatka służbowa i książka służby), zaś w pozostałym zakresie odesłano do odpowiednio: jednolitego rzeczowego wykazu akt – w odniesieniu do okresu przechowywania dokumentacji dotyczącej cudzoziemców umieszczonych w pokoju izolacyjnym oraz zarządzenia wydanego na podstawie art. 5 ust. 3 pkt 5 ustawy z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (t. j. Dz. U. z 2011 r. Nr 171, poz. 1016 z późn. zm.) – w zakresie archiwizowania lub brakowania dokumentacji dotyczącej umieszczenia cudzoziemców w pokoju izolacyjnym (§8 projektu). Tym samym – w ocenie organu do spraw ochrony danych osobowych – w projekcie rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego brak było regulacji w przedmiocie okresu przechowywania dokumentacji dotyczącej osób umieszczonych w pokoju izolacyjnym[290]. W kwestii zaś archiwizowania lub brakowania takiej dokumentacji § 8 ust. 2 projektu rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego odsyłał do aktu prawnego niższego rzędu i to niemającego charakteru powszechnie obowiązującego.

Uwagi Generalnego Inspektora Ochrony Danych Osobowych zostały uwzględnione przez projektodawcę, który w wydanym rozporządzeniu Ministra Spraw Wewnętrznych z dnia 3 czerwca 2013 roku w sprawie pokoju izolacyjnego (Dz. U. z 2013 r. poz. 641) usunął unormowania odnoszące się do prowadzenia monitoringu pokojów izolacyjnych i poprawił przepisy w przedmiocie archiwizowania lub brakowania dokumentacji dotyczącej umieszczania cudzoziemców w takim pokoju.

W 2013 roku zostały podjęte, wnioskowane przez Generalnego Inspektora Ochrony Danych Osobowych od kilku lat, prace legislacyjne zmierzające do dostosowania przepisów ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej (t. j. Dz. U. z 2012 r. poz. 591 z późn. zm.) do – zawartych w Konstytucji Rzeczypospolitej Polskiej i ustawie o ochronie

[289] § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 roku w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych – Dz. U. Nr 248, poz. 1491.
[290] Użyte pojęcie „jednolitego rzeczowego wykazu akt" nie zostało w żaden sposób sprecyzowane w projekcie rozporządzenia Ministra Spraw Wewnętrznych w sprawie pokoju izolacyjnego.

danych osobowych – unormowań odnoszących się do problematyki ochrony danych osobowych. Przygotowany przez Główny Urząd Statystyczny projekt **ustawy o zmianie ustawy o statystyce publicznej**[291] został zasadniczo pozytywnie przyjęty przez GIODO, który wniósł do niego jedynie uwagi o charakterze szczegółowym, akceptując jednocześnie kierunek zaproponowanych zmian.

Generalny Inspektor Ochrony Danych Osobowych zaakcentował wszakże, iż skoro znowelizowana ustawa o statystyce publicznej zawierać będzie katalog danych osobowych, które służby statystyki publicznej mogą przetwarzać[292], to taka konstrukcja poprawionej ustawy o statystyce publicznej rodzić będzie istotną konsekwencję. Otóż brak w wykazie zawartym w projektowanym art. 35 b ust. 1 ustawy o statystyce publicznej, określonej danej osobowej oznaczać będzie, że służby statystyki publicznej nie będą mogły tej danej przetwarzać (a więc pozyskiwać, gromadzić i wykorzystywać dla realizacji swoich zadań), choćby nawet w praktyce okazało się, że jej przetwarzanie jest potrzebne i celowe. Tym samym to na projektodawcy – Głównym Urzędzie Statystycznym – ciąży obowiązek takiego sformułowania katalogu danych w projektowanym art. 35 b ust. 1 ustawy o statystyce publicznej, by zawierał on wszystkie dane niezbędne służbom statystyki publicznej do realizacji ich zadań. W tym kontekście organ do spraw ochrony danych osobowych zwrócił uwagę na nowe brzmienie[293] art. 8 ustawy o statystyce publicznej, który to przepis w projektowanym ust. 1 nie wyłączył możliwości zbierania w trakcie badań statystycznych danych dotyczących pochodzenia etnicznego (narodowości) osób fizycznych, podczas gdy dana taka nie została wymieniona w projektowanym art. 35 b ust. 1 ustawy o statystyce publicznej.

Wątpliwości interpretacyjne wzbudził także nowo wprowadzony[294] ust. 2 art. 8 ustawy o statystyce publicznej. Po stronie organu do spraw ochrony danych osobowych zachodziła niepewność co do relacji zachodzącej między tym przepisem a projektowanym[295] art. 35 b ust. 1 ustawy o statystyce publicznej. Skoro art. 35 b ust. 1 ustawy o statystyce publicznej zawiera katalog danych osobowych, które służby statystyki publicznej mogą przetwarzać, to

[291] DOLiS-033-412/13
[292] Art. 35 b ust. 1 ustawy o statystyce publicznej, dodawany przez art. 1 pkt 20 projektu ustawy o zmianie ustawy o statystyce publicznej.
[293] Nadane przez art. 1 pkt 4 projektu ustawy o zmianie ustawy o statystyce publicznej.
[294] Art. 1 pkt 4 projektu ustawy o zmianie ustawy o statystyce publicznej.
[295] Art. 1 pkt 20 projektu ustawy o zmianie ustawy o statystyce publicznej.

powstaje pytanie, czy unormowanie zamieszczone w art. 8 ust. 2 ww. ustawy[296] nie ma na celu rozszerzenie tego katalogu poprzez dopuszczenie przetwarzania przez służby statystyki publicznej innych danych, aniżeli wymienione w art. 35 b ust. 1 tejże ustawy, w oparciu o dobrowolnie wyrażoną zgodę osoby fizycznej. Zaproponowane[297] ujęcie dyspozycji nowego art. 35 a ust. 1 ustawy o statystyce publicznej zostało przez GIODO uznane za cechujące się pewną niekonsekwencją. Jeśli zamiarem projektodawcy było wprowadzenia do ustawy o statystyce publicznej autonomicznego w stosunku do ustawy o ochronie danych osobowych sposobu rozumienia pojęcia „dane osobowe", to zbędne było – zamieszczone w projektowanym przepisie – sformułowanie „w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926)". W przypadku zaś, gdyby pojęcie „dane osobowe" miało być w znowelizowanej ustawie o statystyce publicznej rozumiane identycznie jak w ustawie o ochronie danych osobowych, niepotrzebne było – użyte w komentowanym przepisie – sformułowanie „jako informacji dotyczących osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania bezpośrednio lub pośrednio, w powiązaniu z danymi o jej życiu i sytuacji". Sformułowanie to stanowi bowiem w takiej sytuacji powtórzenie art. 6 ust. 1 i 2 ustawy o ochronie danych osobowych.

Zasadniczo akceptując sposób unormowania w projekcie obowiązku przekazywania przez podmioty publiczne i podmioty wykonujące zadania publiczne danych dla celów statystyki publicznej (danych administracyjnych), GIODO zakwestionował jednakże projektowany art. 35 c ust. 2 ustawy o statystyce publicznej. Przepis ten, nakładający obowiązek uwzględnienia i określenia zakresu danych podlegających przekazaniu służbom statystyki publicznej ze wszystkich przyszłych urzędowych rejestrów lub systemów informacyjnych, nie mógł być uznany za dopuszczalny. Oprócz oczywistej wadliwości przejawiającej się w fakcie, że nie wskazywał adresata, czyli podmiotu zobligowanego do „uwzględnienia i określenia zakresu danych osobowych, do których zbierania i przetwarzania są uprawnione służby statystyki publicznej", wydawał się on także zupełnie niepotrzebny, albowiem już w projektowanym[298] art. 13 ust. 3 pkt 4 i 5 ustawy o statystyce publicznej przewidziano obowiązek konsultowania z Prezesem Głównego Urzędu Statystycznego nowo tworzonych systemów informacyjnych administracji publicznej i urzędowych rejestrów oraz

[296] Dodawanym przez art. 1 pkt 4 projektu ustawy o zmianie ustawy o statystyce publicznej.
[297] Art. 1 pkt 20 projektu ustawy o zmianie ustawy o statystyce publicznej.
[298] Art. 1 pkt 8 projektu ustawy o zmianie ustawy o statystyce publicznej.

zapewnienia Prezesowi Głównego Urzędu Statystycznego możliwości uczestnictwa w pracach dotyczących tych systemów (rejestrów).

W istniejącym stanie prawnym wypadało organowi do spraw ochrony danych osobowych uznać za kontrowersyjną propozycję zawartą w art. 35 a ust. 4 ustawy o statystyce publicznej, jednakże ostatecznego stanowiska w tej kwestii GIODO nie zajął, gdyż problem proponowanego w tym przepisie wyłączenia miał być rozpatrywany w kontekście planowanej nowelizacji ustawy z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej (t. j. Dz. U. z 2013 r. poz. 672 z późn. zm.), która ma wyłączyć spod regulacji ustawy o ochronie danych osobowych dane przedsiębiorców przetwarzane w Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Wskazane wyżej uwagi GIODO zostały pozytywnie przyjęte przez projektodawcę i uwzględnione w przesłanej do organu do spraw ochrony danych osobowych nowej wersji projektu ustawy o zmianie ustawy o statystyce publicznej[299]. Dlatego Generalny Inspektor Ochrony Danych Osobowych wstępnie zaakceptował przedstawiony wariant brzmienia projektowanego rozdziału 4a ustawy o statystyce publicznej w projekcie ustawy o zmianie ustawy o statystyce publicznej (wersja z dnia 16.09.2013 r.), zastrzegając wszakże ponownie[300], że organ do spraw ochrony danych osobowych będzie traktował katalog z projektowanego art. 35 b ust. 1 ustawy o statystyce publicznej jako zamknięty. Co za tym idzie, brak wymienienia w przedmiotowym katalogu określonej danej osobowej oznaczać będzie (po wejściu w życie znowelizowanej ustawy o statystyce publicznej) zakaz przetwarzania takiej danej o osobie fizycznej przez służby statystyki publicznej.

Oprócz powyższego organ do spraw ochrony danych osobowych wniósł, by w projektowanym art. 35 b ust. 1 ustawy o statystyce publicznej wprost zawrzeć stwierdzenie, że służby statystyki publicznej są uprawnione do pozyskiwania do celów statystycznych informacji o niepełnosprawności i danych o stanie zdrowia, skoro w projektowanym art. 35 b ust. 2 pkt 11 i 32 ustawy przewidziano prowadzenie badań statystycznych dotyczących tych zagadnień. Prace legislacyjne dotyczące projektu ustawy o zmianie ustawy o statystyce publicznej były kontynuowane w 2014 roku, kiedy to została opracowana ostateczna wersja tego projektu.

[299] Pismo Prezesa GUS z dnia 8 listopada 2013 roku – znak: GP-11-024-105/36/2013.
[300] Pismo z dnia 10 grudnia 2013 roku o sygn. DOLiS-033-412/13/TG/82659.

O ile współpracę między Głównym Urzędem Statystycznym a Generalnym Inspektorem Ochrony Danych Osobowych przy projekcie ustawy o zmianie ustawy o statystyce publicznej uznać wypada za wzorcową, to organy te pozostawały ze sobą w zasadniczym sporze w odniesieniu do projektu **rozporządzenia Prezesa Rady Ministrów zmieniającego rozporządzenie 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**[301]. Organ do spraw ochrony danych osobowych wniósł bowiem zasadnicze zastrzeżenia wobec propozycji brzmienia działu VIII. AKTYWNOŚĆ EKONOMICZNA, proponowanego w tym projekcie, formularza „R-SGR – Badanie struktury gospodarstw rolnych".

W kwestionowanej części projektowanego formularza „R-SGR – Badanie struktury gospodarstw rolnych" znalazło się bowiem pytanie w kwestii pozostawania respondenta w związku partnerskim (pkt 1), jak również dalsze pytania zmierzające do bliższego scharakteryzowania partnera (partnerki) respondenta (pkt 5a – 14b). Przypomnieć zaś należy, że z prawa służb statystyki publicznej do zbierania informacji o datach zawarcia i ustania małżeństw[302] - statuowanego w obowiązującym art. 35 ust. 1 pkt 6 ustawy o statystyce publicznej - w żadnym razie nie można wywodzić uprawnienia tych służb do pozyskiwania informacji tego samego rodzaju w odniesieniu do związków partnerskich. Informacja o pozostawaniu w związku partnerskim należy do najintymniejszej sfery życia prywatnego i rodzinnego osoby fizycznej i legalne przetwarzanie takiej danej przez służby statystyki publicznej wymagałoby jednoznacznego upoważnienia ich do tego rodzaju działań w przepisie prawa rangi ustawowej (art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych). Wobec braku takiego przepisu ustawy, unormowanie zaproponowane w dziale VIII. AKTYWNOŚĆ EKONOMICZNA projektowanego formularza „R-SGR – Badanie struktury gospodarstw rolnych" stanowi naruszenie – gwarantowanego przez Konstytucję Rzeczypospolitej Polskiej – prawa osoby fizycznej do prywatności (art. 47) i ochrony dotyczących jej danych osobowych (art. 51), jak również zasad ochrony danych osobowych określonych w ustawie o ochronie danych osobowych.

[301] DOLiS-033-481/13
[302] Dla celów statystycznych i przygotowania prognoz demograficznych.

Z uwagi na powyższe GIODO zażądał usunięcia z działu VIII. AKTYWNOŚĆ EKONOMICZNA projektowanego formularza „R-SGR – Badanie struktury gospodarstw rolnych" zawartego w projekcie omawianego rozporządzenia, wszystkich pytań dotyczących nieformalnych związków osoby objętej badaniem statystycznym.

Wobec odmowy ze strony Prezesa Głównego Urzędu Statystycznego[303], GIODO ponownie podniósł[304], iż obowiązujące przepisy ustawy o statystyce publicznej nie upoważniają tych służb do gromadzenia informacji o pozostawaniu przez użytkownika gospodarstwa rolnego w związku niesformalizowanym[305]. Tym samym – w świetle dyspozycji art. 7 Konstytucji Rzeczypospolitej Polskiej nakładającego na organy władzy publicznej[306] obowiązek działania na podstawie i w granicach prawa – brak jest prawnej legitymizacji dla prowadzenia „szerokich analiz poziomu występowania tego zjawiska", w oparciu o przymusowe ankiety wypełniane przez respondentów. GIODO zauważył również, iż kwestionowany formularz „R-SGR – Badanie struktury gospodarstw rolnych" w dziale VIII. AKTYWNOŚĆ EKONOMICZNA przewiduje zbieranie numerów PESEL osób pozostających w związkach z użytkownikami gospodarstw rolnych, a zatem dopuszczenie przez Generalnego Inspektora Ochrony Danych Osobowych jego stosowania przez służby statystyki publicznej, w powiązaniu z faktem dostępu tych służb do zbioru PESEL, skutkowałoby powstaniem w Głównym Urzędzie Statystycznym zbioru danych osób pozostających w związkach niesformalizowanych z użytkownikami gospodarstw rolnych. Utworzenie zaś takiego zbioru przez Główny Urząd Statystyczny wymagałoby legitymowania się przez ten Urząd upoważnieniem zawartym w przepisie ustawy[307].

Według stanu na czerwiec 2014 roku sprzeciw GIODO w stosunku do formularza „R-SGR – Badanie struktury gospodarstw rolnych" zawartego w projekcie rozporządzenia Prezesa Rady Ministrów zmieniającego rozporządzenie 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 był skuteczny, gdyż projekt ten nie został jeszcze podpisany przez Prezesa Rady Ministrów.

[303] Pismo Prezesa GUS z dnia 26 listopada 2013 roku – znak: PK-02-4201-124/2013.
[304] Pismo z dnia 12 grudnia 2013 roku o sygn. DOLiS-033-481/13/TG/83572.
[305] Nazwanym w badaniu „R-SGR – Badanie struktury gospodarstw rolnych" związkiem partnerskim
[306] W tym Główny Urząd Statystyczny.
[307] Art. 27 ust. 2 pkt 2 w zw. z ust. 1 ustawy o ochronie danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych przyjął z zadowoleniem podjęcie w 2013 roku przez projektodawcę działań legislacyjnych zmierzających do zapewnienia, sprawowanej przez niezależny i autonomiczny organ, zewnętrznej kontroli przetwarzania danych przez służby specjalne, gdyż na potrzebę istnienia takiej kontroli zwracał uwagę już od kilku lat. Jednakże kierunkowa aprobata dla poczynań projektodawcy uzewnętrznionych w projekcie **ustawy o Komisji Kontroli Służb Specjalnych**[308] nie oznaczała całościowego zaakceptowania jego postanowień. Niektóre z zaproponowanych unormowań rodziły bowiem poważne wątpliwości co do ich wyczerpującego charakteru i zgodności z standardami europejskim w zakresie ochrony danych osobowych i prawa do prywatności.

W pierwszej kolejności niemożliwe do zaakceptowania dla organu do spraw ochrony danych osobowych było – przewidziane w art. 1 ust. 1 pkt 1 lit. b projektu – ograniczenie kontroli sprawowanej przez Komisję Kontroli Służb Specjalnych do danych osobowych obywateli Rzeczypospolitej Polskiej. Ograniczenie takie nie znajduje podstaw zarówno w art. 51 Konstytucji Rzeczypospolitej Polskiej, jak i w aktach prawnych przyjętych na poziomie europejskim. Artykuł 1 Konwencji Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja Nr 108), podpisanej w Strasburgu dnia 28 stycznia 1981 roku, wyraźnie wskazuje, że ma ona na celu zagwarantowanie, na terytorium każdej ze stron, każdej osobie fizycznej, niezależnie od jej narodowości i miejsca zamieszkania, poszanowania jej praw i podstawowych wolności, w szczególności prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych („ochrona danych"). Również protokół dodatkowy z dnia 8 listopada 2001 roku do Konwencji Nr 108, dotyczący organów nadzoru i transgranicznych przepływów danych, określając zakres kompetencji organów nadzorczych w odniesieniu do rozpatrywania skarg wyraźnie wskazuje, że mogą być one wnoszone przez jakąkolwiek osobę. Jednocześnie GIODO podkreślił, że ograniczenie kontroli sprawowanej przez Komisję Kontroli Służb Specjalnych do danych osobowych obywateli Rzeczypospolitej Polskiej z jednej strony – w dużym stopniu wyłączyłoby kontrolę wspomnianej Komisji nad przetwarzaniem danych przez niektóre służby specjalne wymienione w projekcie ustawy o Komisji Kontroli Służb Specjalnych, z drugiej zaś – powodowałoby trudności praktyczne

[308] DOLiS-033-442/13

we właściwym wyodrębnieniu danych dotyczących obywateli i nie obywateli Rzeczypospolitej Polskiej w zbiorach danych służb specjalnych.

Po drugie, Komisja Kontroli Służb Specjalnych (z pewnymi zastrzeżeniami) nie ma uprawnień władczych, a jedynie kompetencje kontrolne. Oprócz postępowań kontrolnych jest ona wprawdzie uprawniona do rozpatrywania skarg na działalność służb specjalnych[309], ale – w myśl art. 61 projektu – jedynie przesłanych za pośrednictwem podmiotów wymienionych w art. 3 ust. 1 projektu. Do rozpatrywania takich skarg stosuje się przepisy art. 227 – 240 ustawy z dnia 14 czerwca 1960 roku – Kodeks postępowania administracyjnego (Dz. U. z 2013 r. poz. 267 z późn. zm.), czyli tryb postępowania w sprawach skargi powszechnej. Takie ukształtowanie kompetencji Komisji Kontroli Służb Specjalnych powoduje, że nie może być ona traktowana jako organ nadzorczy, o którym mowa we ww. protokole dodatkowym do Konwencji Nr 108[310]. Organ nadzorczy w rozumieniu protokołu dodatkowego, powinien między innymi rozpatrywać skargi wnoszone przez jakąkolwiek osobę dotyczące ochrony jej praw i podstawowych wolności w związku z przetwarzaniem danych osobowych, w zakresie swej kompetencji[311]. Ponadto od decyzji organu nadzorczego w rozumieniu protokołu dodatkowego, która daje podstawy do zaskarżenia, powinno przysługiwać odwołanie do sądu. Tymczasem projekt ustawy o Komisji Kontroli Służb Specjalnych nie przewiduje takich rozwiązań. Tym samym – w ocenie Generalnego Inspektora Ochrony Danych Osobowych – w odniesieniu do zakresu działania i kompetencji Komisji Kontroli Służb Specjalnych projekt ten nie zapewnia spełnienia standardów prawa europejskiego wynikających z Konwencji Nr 108 oraz protokołu dodatkowego do Konwencji Nr 108 dotyczącego organów nadzoru i transgranicznych przepływów danych. Wątpliwości budził także – określony w art. 1 ust. 1 pkt 1 zdanie wstępne projektu ustawy o Komisji Kontroli Służb Specjalnych – zakres podmiotowy właściwości Komisji Kontroli Służb Specjalnych. Z nieznanych organowi do spraw ochrony danych osobowych powodów,

[309] Rozdział 4 projektu ustawy o Komisji Kontroli Służb Specjalnych.

[310] Zgodnie z art. 1 ust. 2 lit. a protokołu dodatkowego z dnia 8 listopada 2001 roku do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, dotyczącym organów nadzoru i transgranicznych przepływów danych, krajowe organy nadzorcze powinny mieć w szczególności uprawnienia dochodzeniowe i interwencyjne, jak również prawo do angażowania się w postępowanie prawne lub informowania właściwych organów sądowych o naruszeniach przepisów prawa krajowego, realizując zasady określone w rozdziałach II i III Konwencji Nr 108 oraz w protokole dodatkowym.

[311] Art. 1 ust. 1 lit. b protokołu dodatkowego z dnia 8 listopada 2001 roku do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, dotyczący organów nadzoru i transgranicznych przepływów danych.

wymieniony w tym przepisie katalog podmiotów, które mogą podlegać kontroli Komisji Kontroli Służb Specjalnych, nie obejmuje wywiadu skarbowego, o którym mowa w rozdziale 4 ustawy z dnia 28 września 1991 roku o kontroli skarbowej (t. j. Dz. U. z 2011 r. Nr 41, poz. 214 z późn. zm.)[312]. Co więcej, rozwiązanie zaproponowane w art. 1 ust. 1 projektu, z jednej strony pozostawia np. Policję poza zakresem podmiotowym kontroli sprawowanej przez Komisję Kontroli Służb Specjalnych, a jednocześnie nie odnosi się do kwestii sposobu kontrolowania przetwarzania danych w zbiorach danych zawierających informacje niejawne, w stosunku do których to zbiorów kompetencje kontrolne Generalnego Inspektora Ochrony Danych Osobowych są wyłączone na podstawie art. 43 ust. 2 ustawy o ochronie danych osobowych.

Poza podniesionymi wyżej zastrzeżeniami o charakterze zasadniczym GIODO stwierdził także, że poprawienia wymaga art. 27 projektowanej ustawy dotyczący składania oświadczeń majątkowych przez członków Komisji Kontroli Służb Specjalnych, a także dyrektora i pracowników Biura Komisji Kontroli Służb Specjalnych. Uwzględniając, że zarówno ustawa o ochronie danych osobowych, jak i dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[313], statuują tzw. zasadę ograniczenia czasowego, zgodnie z którą administrator danych powinien zapewnić, aby wykonywanie przez niego na danych osobowych operacji odbywało się nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania[314], nietrafne jest zaproponowane rozwiązanie, zgodnie z którym każde złożone przez członka Komisji Kontroli Służb Specjalnych, dyrektora Biura Komisji Kontroli Służb Specjalnych oraz pracownika Biura Komisji Kontroli Służb Specjalnych oświadczenie majątkowe ma być włączane do jego akt osobowych, a tym samym przechowywane właściwie bezterminowo. Projektodawca nie wskazał w uzasadnieniu projektu przyczyn, dla których zdecydował się na taką konstrukcję powyższego przepisu, odmienną w stosunku do unormowań dotyczących kwestii składania oświadczeń majątkowych zawartych w innych ustawach, w których wprost wskazuje się okresy ich przechowywania. Organ do spraw ochrony danych osobowych pozostawił pod

[312] Pominięcie to wydaje się tym bardziej niezrozumiałe, jeśli zauważyć, że wywiad skarbowy posiada w zasadzie te same kompetencje co służby specjalne wskazane w art. 1 ust. 1 pkt 1 zdanie wstępne projektu ustawy o Komisji Kontroli Służb Specjalnych.
[313] Dz. Urz. WE L 281 z 23.11.1995, str. 31 z późn. zm.
[314] Odpowiednio art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych oraz art. 6 ust. 1 lit. e dyrektywy 95/46/WE.

rozwagę projektodawcy również kwestię, czy wzgląd na stosowane przez kontrolowane służby specjalne zaawansowane środki nowych technologii nie przemawia za wprowadzaniem wymagania, by przynajmniej niektórzy członkowie Komisji Kontroli Służb Specjalnych legitymowali się innym specjalistycznym wykształceniem (np. informatycznym), bądź by ograniczenie dotyczące wyższego wykształcenia prawniczego stosować jedynie do części (np. połowy) składu Komisji Kontroli Służb Specjalnych. Takie specjalistyczne wykształcenie niektórych członków Komisji Kontroli Służb Specjalnych mogłoby zwiększyć skuteczność kontroli nad narzędziami informatycznymi i innymi środkami, którymi służby specjalne się posługują.

Z informacji uzyskanych przez GIODO wynika, że od października 2013 roku prace legislacyjne dotyczące projektu ustawy o Komisji Kontroli Służb Specjalnych toczą się bardzo powoli.

W 2013 roku trwały prace dotyczące zmian ustawy o ochronie danych osobowych zawartych w projekcie **ustawy o ułatwieniu wykonywania działalności gospodarczej**[315]. Wskazać wszakże należy, iż miały one głównie charakter uzgodnień roboczych między Ministrem Gospodarki (autorem projektu ustawy o ułatwieniu wykonywania działalności gospodarczej) a Generalnym Inspektorem Ochrony Danych Osobowych oraz polegały na udzielaniu przez GIODO odpowiedzi na pytania podmiotów zainteresowanych różnymi aspektami nowelizacji ustawy o ochronie danych osobowych. Ostateczna wersja zmian ustawy o ochronie danych osobowych została sporządzona w roku 2014. Odnotować wszakże wymaga, że w związku z uwagami do projektowanego art. 8 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej zgłoszonymi na konferencji uzgodnieniowej w dniu 9 grudnia 2013 roku, Generalny Inspektor Ochrony Danych Osobowych przedłożył wyjaśnienia i propozycje kompromisowe. W piśmie z dnia 17 grudnia 2013 r.[316] stwierdził, że w kontekście wątpliwości co do wzajemnego stosunku – wykonywanego przez administratora bezpieczeństwa informacji – sprawdzenia, o którym mowa w art. 16a ustawy o ochronie danych osobowych[317] i sprawdzenia z art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych[318] wyjaśnić należy, że są to dwie różne instytucje prawne. W pierwszym

[315] DOLiS-033-450/13
[316] DOLiS-033-450/13/TG/84644
[317] Dodawanym przez art. 8 pkt 2 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[318] Ibidem

przypadku administrator bezpieczeństwa informacji dokonuje sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych u administratora danych, który go powołał, na zlecenie Generalnego Inspektora Ochrony Danych Osobowych. W konsekwencji sprawozdanie z takiego sprawdzenia jest przedstawiane, za pośrednictwem administratora danych, Generalnemu Inspektorowi Ochrony Danych Osobowych. W drugim zaś przypadku (art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych) sprawdzenie przeprowadzane przez administratora bezpieczeństwa informacji ma charakter kontroli wewnętrznej u administratora danych, a zatem powstałe w jego wyniku sprawozdanie jest dokumentem wewnętrznym administratora danych. Przedmiotowe kwestie zostaną szczegółowo uregulowane w rozporządzeniu, który będzie wydany na podstawie delegacji zamieszczonej w art. 36a ust. 7 pkt 1 ustawy o ochronie danych osobowych.

Wychodząc naprzeciw argumentom co do potrzeby umożliwienia administratorom danych dostosowania się do nowych unormowań dotyczących administratorów bezpieczeństwa informacji[319], Generalny Inspektor Ochrony Danych Osobowych wnioskował o wydłużenie do 6 miesięcy od dnia wejścia w życie projektowanej ustawy o ułatwieniu wykonywania działalności gospodarczej *vacatio legis* dla przepisów zamieszczonych w art. 8 pkt 1 – 7 tejże ustawy. Ponadto podtrzymał[320] stanowisko co do potrzeby dodania w art. 36a ust. 7 pkt 1 ustawy o ochronie danych osobowych[321], po słowie „tryb" sformułowania „i sposób". Proponowana poprawka miała na celu nałożenie na ministra właściwego do spraw administracji publicznej obowiązku określenia w rozporządzeniu sposobu wykonywania przez administratorów bezpieczeństwa informacji ich zadań, o których mowa w art. 36a ust. 2 pkt 1 lit. a i b ustawy o ochronie danych osobowych[322], a tym samym – ułatwienie funkcjonowania administratorom bezpieczeństwa informacji poprzez jednoznaczne wskazanie obowiązków, które ciążą na nich w procesie zapewnienia u danego administratora danych zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

[319] Chodzi o wymagania formalne z art. 36a ust. 4 ustawy o ochronie danych osobowych oraz bezpośrednie podporządkowanie administratora bezpieczeństwa informacji kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych z art. 36a ust. 6 tejże ustawy.
[320] Wyrażone w piśmie z dnia 5 listopada 2013 roku o sygn. DOLiS-033-450/13/TG/72911.
[321] Dodawanym przez art. 8 pkt 4 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[322] Dodawanym przez art. 8 pkt 4 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).

Wzgląd na deregulacyjny charakter projektowanej ustawy o ułatwieniu wykonywania działalności gospodarczej przemawiał również za wydłużeniem do 30 dni, przewidzianego w art. 46b ust. 1 ustawy o ochronie danych osobowych[323], terminu na zgłoszenie Generalnemu Inspektorowi Ochrony Danych Osobowych przez administratora danych powołania (odwołania) administratora bezpieczeństwa informacji. To przedłużenie czasu ma istotne znaczenie dla administratorów danych, gdyż w okresie pomiędzy dokonaniem czynności odwołania administratora bezpieczeństwa informacji a jej zgłoszeniem Generalnemu Inspektorowi Ochrony Danych Osobowych administrator danych może korzystać ze zwolnienia z obowiązku zgłoszenia do rejestracji zbiorów danych osobowych, o którym mowa w art. 43 ust. 1a ustawy o ochronie danych osobowych. Z tych samych przyczyn organ do spraw ochrony danych osobowych zrezygnował z – przewidzianego w art. 46d ust. 3 ustawy o ochronie danych osobowych – rygoru natychmiastowej wykonalności w odniesieniu do decyzji o wykreśleniu administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji. Zmiana ta umożliwi administratorowi danych, w okresie pomiędzy wydaniem przez Generalnego Inspektora Ochrony Danych Osobowych decyzji o wykreśleniu administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji a uzyskaniem przez tę decyzję przymiotu ostateczności, korzystanie ze zwolnienia z obowiązku zgłoszenia do rejestracji prowadzonych zbiorów danych osobowych (w zakresie przewidzianym w art. 43 ust. 1a ustawy o ochronie danych osobowych[324]). W przypadku przyjęcia tej poprawki stosownej zmiany wymagać będzie dyspozycja art. 46d ust. 3 ustawy o ochronie danych osobowych[325].

Generalny Inspektor Ochrony Danych Osobowych oponował także przeciwko propozycji, by przewidziany w art. 46c ustawy o ochronie danych osobowych[326] ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji nie zawierał ich imion i nazwisk. W opinii organu do spraw ochrony danych osobowych usunięcie powyższych danych z przedmiotowego rejestru skutkowałoby zmianą jego charakteru. Rejestr

[323] Dodawanym przez art. 8 pkt 7 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[324] Dodawanym przez art. 8 pkt 6 lit. b projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[325] Dodawanego przez art. 8 pkt 7 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[326] Dodawany przez art. 8 pkt 7 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).

ten przestałby być rejestrem administratorów bezpieczeństwa informacji, a stałby się rejestrem administratorów danych, którzy zgłosili Generalnemu Inspektorowi Ochrony Danych Osobowych administratorów bezpieczeństwa informacji. Co więcej, postulowany brak w rejestrze administratorów bezpieczeństwa informacji ich imion i nazwisk istotnie utrudniałby osobom zainteresowanym kontakt z tymi administratorami. Natomiast celem objęcia zakresem art. 46d ustawy o ochronie danych osobowych (dotyczącego wykreślania administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji) wszystkich możliwych przypadków Generalny Inspektor Ochrony Danych Osobowych wnioskował o uzupełnienie dyspozycji art. 46d ust. 1 ustawy o ochronie danych osobowych (*in fine*) o sformułowanie: „albo w przypadku jego śmierci".

Podkreślenia wymaga, że organ do spraw ochrony danych osobowych nie podzielił wyrażanych na konferencji uzgodnieniowej w dniu 9 grudnia 2013 roku przez Polską Agencję Rozwoju Przedsiębiorczości (PARP) wątpliwości, co do sposobu rozumienia art. 46e ust. 2 ustawy o ochronie danych osobowych. W opinii GIODO - wobec uzupełnienia na ww. konferencji dyspozycji art. 46e ust. 1 ustawy o ochronie danych osobowych[327] część wstępna o sformułowanie „ponownego" (po sformułowaniu „W przypadku") – jedynym możliwym kierunkiem wykładni art. 46e ust. 2 ustawy o ochronie danych osobowych[328] jest przyjęcie, iż przepis ten (w odniesieniu do kwestii zwolnienia z obowiązku rejestracji zbiorów danych osobowych) dotyczy wyłącznie sytuacji, gdy administrator danych ponownie zgłasza Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji administratora bezpieczeństwa informacji, który został uprzednio wykreślony z rejestru administratorów bezpieczeństwa informacji w trybie określonym w art. 46d ust. 2 ustawy o ochronie danych osobowych. Za takim stanowiskiem Generalnego Inspektora przemawia zarówno umiejscowienie art. 46e ust. 2 ustawy o ochronie danych osobowych w projektowanych zmianach ustawy o ochronie danych osobowych, jak i porównanie jego brzmienia z ujęciem dyspozycji ustępu 1 tego przepisu oraz brzmieniem art. 43 ust. 1a ustawy o ochronie danych osobowych[329]. Wobec podnoszonych na konferencji uzgodnieniowej niejasności co do stanowiska Generalnego Inspektora Ochrony Danych Osobowych, organ do spraw ochrony

[327] Dodawanego przez art. 8 pkt 7 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[328] Dodawanego przez art. 8 pkt 7 projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).
[329] Dodawanego przez art. 8 pkt 6 lit. b projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (wersja z dnia 02.10.2013 r.).

danych osobowych wniósł o zamieszczenie w uzasadnieniu projektu ustawy o ułatwieniu wykonywania działalności gospodarczej wyjaśnienia, że celem zmian zaproponowanych w art. 8 pkt 8 projektu z dnia 02.10.2013 r. jest przystąpienie przez polski organ do spraw ochrony danych osobowych do procedury wzajemnego uznawania (ang. MUTUAL RECOGNITION). Z tych samych, co powyższe, przyczyn Generalny Inspektor Ochrony Danych Osobowych wniósł także o uzupełnienie uzasadnienia projektu ustawy o ułatwieniu wykonywania działalności gospodarczej o wyjaśnienie, że nie oponuje przeciwko outsourcing´owi zadań administratora bezpieczeństwa informacji przez administratora danych i przedmiotowy projekt ustawy działań takich nie zakazuje.

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

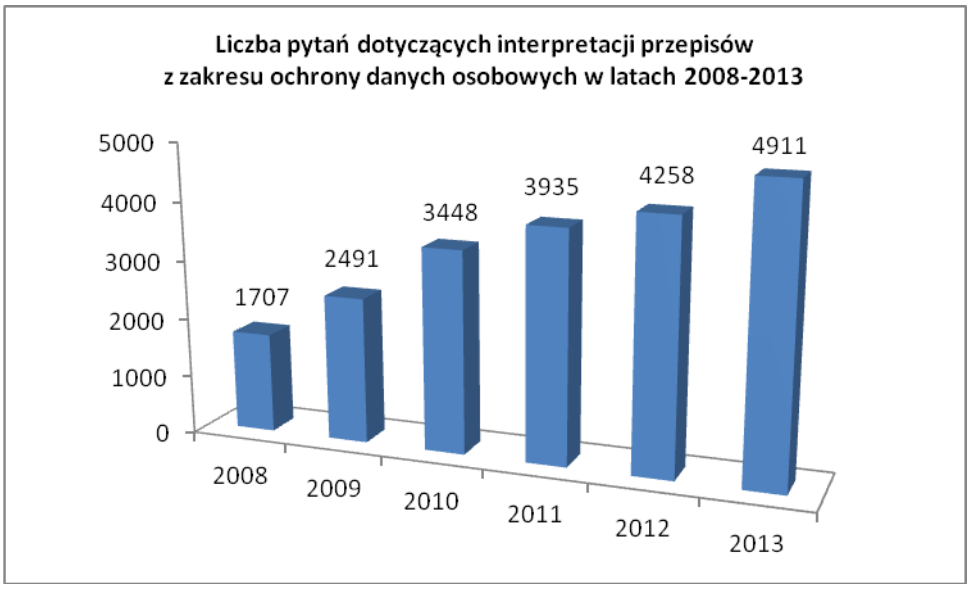
Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych, stanowi bardzo ważną część działalności Generalnego Inspektora Ochrony Danych Osobowych. Działania te obejmują szeroko zakrojone działania informacyjne i edukacyjne, których różnorodna forma i dynamika ma wpływ na podnoszenie świadomości społecznej w sprawach dotyczących prawa do prywatności i ochrony danych osobowych.

8.1. Interpretacja przepisów

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 2013 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **4911 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 2012 wpłynęło 4258 pytań prawnych z zakresu ochrony danych osobowych, zaś w 2011 r. – 3935, 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 2008–2013 przedstawia poniższy wykres.



Wykres 37: ***Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach 2008–2013.***

Powyższy wykres ilustruje zauważalną z roku na rok tendencję wzrostową wpływu pytań prawnych kierowanych do GIODO, co przekłada się na wydłużenie okresu udzielania na nie odpowiedzi.

W porównaniu z ubiegłym rokiem, w okresie objętym niniejszym *Sprawozdaniem* o **653 zwiększyła się liczba pytań**, które w 2013 r. wpłynęły do organu do spraw ochrony danych osobowych. Nadawcami największej liczby pytań były osoby fizyczne, w tym osoby prowadzące działalność gospodarczą. Stąd należy wnosić, że działania o charakterze informacyjnym i edukacyjnym realizowane przez organ do spraw ochrony danych osobowych potrzebne są w szczególności osobom, które nie korzystają na co dzień z profesjonalnej pomocy prawnej. W celu promocji wiedzy na temat ochrony danych osobowych pracownicy Biura GIODO udzielali odpowiedzi na pytania zarówno w formie pisemnej, jak i ustnej w ramach codziennych konsultacji w siedzibie Biura.

Przedstawiona poniżej analiza **pytań prawnych**, które w 2013 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 oraz przetwarzaniem danych osobowych przez związki zawodowe i w stosunkach pracy.

8.1.1. Administracja publiczna

Wiele wątpliwości osób kierujących pytania do Generalnego Inspektora Ochrony Danych Osobowych budziły **kwestie związane ze stosowaniem ustawy o utrzymaniu czystości i porządku w gminach.**

Jako przykład można wskazać zapytanie jednego z przedsiębiorstw wodociągowo-kanalizacyjnych w kwestii, czy jest ono uprawnione do **udostępnienia gminie danych dotyczących ilości zużytej przez mieszkańców wody oraz adresu nieruchomości w celu ustalenia przez gminę wysokości opłaty za gospodarowanie odpadami komunalnymi**[330]**.**

W odpowiedzi Generalny Inspektor poinformował, że tryb i zasady prowadzenia zadań gminy w zakresie utrzymania czystości i porządku w gminach określone są przepisami ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2012 r. poz. 391 z późn. zm.). Przepisy tej ustawy wskazują zasady przetwarzania danych osobowych do konkretnych, określonych w tej ustawie celów. Wskazał też, że przepisy ww. ustawy (dokładnie zaś art. 6m ust. 1) obligują w pierwszej kolejności właścicieli nieruchomości do złożenia do wójta, burmistrza lub prezydenta miasta deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w terminie 14 dni od dnia zamieszkania na danej nieruchomości pierwszego mieszkańca lub powstania na danej nieruchomości odpadów komunalnych, przy czym każda zmiana informacji będących podstawą ustalania wysokości należnej opłaty stanowi podstawę do wypełnienia i dostarczenia właściwym organom nowej deklaracji (ust. 2).

Przepisy ustawy o utrzymaniu czystości i porządku w gminach przewidują także tryb postępowania w sytuacji, gdy deklaracja nie zostanie złożona albo zaistnieją uzasadnione wątpliwości co do danych zawartych w deklaracji (art. 6o i kolejne) stanowiąc o określeniu, w drodze decyzji, wysokości zaległości z tytułu opłaty za gospodarowanie odpadami komunalnymi. Oznacza to, że dla takich sytuacji, w trybie postępowania administracyjnego,

[330] DOLiS-035-753/13

możliwym jest pozyskanie przez gminę informacji koniecznych dla ustalenia stanu faktycznego przed wydaniem właściwej decyzji. Przesłanką legalności udostępnienia danych gminie w przedmiotowym przypadku może być ta, o której mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Przepis ten stanowi bowiem, iż przetwarzanie danych (w tym także ich udostępnianie) jest dopuszczalne, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Przepisy te natomiast ujęte są w ustawie z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 2013 r. poz. 267), gdy przetwarzanie danych osobowych będzie zachodzić w drodze stosownego postępowania zmierzającego do ustalenia obowiązku uiszczenia opłaty za gospodarowanie odpadami komunalnymi. Udostępnienie danych osobowych dla celu prowadzonego postępowania może nastąpić jedynie o ile jest niezbędne dla takiego postępowania, a zatem ściśle związane z przedmiotem postępowania (i jego stroną/stronami w rozumieniu ustawy Kodeks postępowania administracyjnego) i tylko w takim zakresie, jakiego dotyczy to postępowanie, a w przypadku gdy z żądaniem udostępnienia występuje podmiot (organ) związany przepisami prawa, to jedynie z granicach tych przepisów, czy wyznaczonych ww. przepisami szczególnymi kompetencji.

Kolejne pytanie dotyczące stosowania przepisów o utrzymaniu czystości i porządku w gminach dotyczyło **możliwości przekazania przez gminę danych ze zbiorów meldunkowych spółce wodociągowo-kanalizacyjnej w celu realizacji zadań z ustawy o utrzymaniu czystości i porządku w gminie**[331]. W odpowiedzi poinformowano, że ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (t.j. Dz. U. 2006 r. Nr 139, poz. 993 z późn. zm.) w Rozdziale 8b „Udostępnianie danych osobowych ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych", określa tryb i zasady udostępniania informacji – w tym danych osobowych – z tych zbiorów. Artykuł 44h ust. 1 pkt 4 ww. ustawy stanowi, iż dane ze zbiorów meldunkowych, zbioru PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, państwowym i komunalnym jednostkom organizacyjnym oraz innym podmiotom w zakresie niezbędnym do realizacji zadań publicznych określonych w odrębnych przepisach. Zgodnie natomiast z art. 44i ust. 1 ustawy o ewidencji ludności i dowodach osobistych, dane ze

[331] DOLiS-035-1646/13

zbiorów meldunkowych oraz ewidencji wydanych i unieważnionych dowodów osobistych udostępnia organ gminy. Zastosowanie dla przedmiotowej sytuacji będą mogły mieć tryb i zasady udostępniania danych określone w 44h ust. 3 i 5 oraz w wydanym na podstawie art. 44h ust. 8 akcie wykonawczym.

Biorąc pod uwagę treść powyższych przepisów należało podkreślić, że dla udostępnienia przez gminę „meldunkowej bazy danych dotyczących właścicieli nieruchomości" musiałoby istnieć przyzwolenie ustawodawcy w jasno i precyzyjnie taką możliwość dopuszczających przepisach prawa. Takie przyzwolenie jednak nie istnieje. Ustawodawca precyzyjnie bowiem wskazuje, iż udostępnienie może dotyczyć jedynie określonych danych, w trybie wnioskowym, przy możliwości korzystania z elektronicznych form przetwarzania danych z zapewnieniem odpowiednich metod technicznych i organizacyjnych służących szeroko rozumianemu zabezpieczeniu danych.

Jednostka komunalna może posiadać umocowanie do przetwarzania danych osobowych w przepisach rangi ustawy. W przedmiotowej sytuacji wątpliwa była jednak przydatność pozyskiwanych ze zbiorów meldunkowych danych (w całości) dla realizacji celów określonych przepisami ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2012 r. poz. 391 z późn. zm.). Zwłaszcza, iż zbiory te nie zawierają informacji służących wprost ustaleniu właścicieli nieruchomości w rozumieniu przepisów wspomnianej ustawy. Jak stanowi art. 2 ust. 1 pkt 4 ustawy o utrzymaniu czystości i porządku w gminach, ilekroć w tej ustawie jest mowa o właścicielach nieruchomości, rozumie się przez to także współwłaścicieli, użytkowników wieczystych oraz jednostki organizacyjne i osoby posiadające nieruchomości w zarządzie lub użytkowaniu, a także inne podmioty władające nieruchomością. Innymi słowy, administrator danych – przetwarzając dane osobowe – jest zobligowany tak zorganizować ten proces, aby działać zgodnie z powszechnie obowiązującymi przepisami prawa, w tym z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi. Udostępnianie danych przez podmioty zobowiązane do działania w granicach kompetencji nadanych im mocą stosownych przepisów, musi znajdować podstawę w wyraźnie i jednoznacznie określonych przepisach prawa, zarówno w zakresie przedmiotowym (czyli jaki zakres danych miałby podlegać upublicznieniu) oraz podmiotowym (czyli komu – jakim osobom, instytucjom – miałyby zostać udostępnione oraz w jakim celu).

Do grupy pytań dotyczących realizacji zadań gmin zaliczyć można zapytanie dotyczące **opieki nad zwierzętami bezdomnymi jako zadania własnego gminy**. Wyłapywanie bezdomnych zwierząt i zapewnienie im miejsca w schroniskach często zlecane jest przez gminy podmiotom gospodarczym. Pytanie skierowane do Generalnego Inspektora Ochrony Danych przez jedną z osób zaniepokojoną sposobem wykonywania powyższego, finansowanego ze środków komunalnych, zadania przez jedno ze schronisk dla zwierząt, dotyczyło **możliwości zapoznania się przez osoby zainteresowane z wykazem nowych właścicieli psów pochodzących z tego schroniska**[332].

W odpowiedzi Biuro GIODO poinformowało, że działalność podmiotów gospodarczych w zakresie, w jakim wykorzystują one majątek lub środki państwowe lub komunalne oraz wywiązują się z zobowiązań finansowych na rzecz państwa może być przedmiotem kontroli Najwyższej Izby Kontroli. Postępowanie kontrolne oraz uprawnienia inspektorów NIK, które obejmują również dostęp do potrzebnych dla celów kontrolnych informacji, uregulowane zostały w ustawie o Najwyższej Izbie Kontroli w z dnia 23 grudnia 1994 r. (Dz. U. z 2012, poz. 820 z późn. zm.).

Z kolei pytanie pochodzące od jednostki administracji publicznej dotyczyło zagadnienia, **w jaki sposób powinien postąpić zespół przeprowadzający nabór na stanowisko w służbie celnej z ofertą (aplikacją) kandydata niezawierającą zgody na przetwarzanie danych osobowych**[333].

W odpowiedzi na to zapytanie poinformowano, że zgoda osoby, której dane dotyczą, określona – odpowiednio – w art. 23 ust. 1 pkt 1 oraz art. 27 ust. 2 pkt 1, jak z powyższego wynika, nie jest jedyną podstawą upoważniającą do przetwarzania danych osobowych. Ustawodawca zastrzegł także możliwość działania przez podmiot pozyskujący dane osobowe na podstawie przepisów prawa. Przy czym w odniesieniu do danych wrażliwych – wymaga istnienia przepisów rangi ustawy stwarzających pełne gwarancje ochrony danych (art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy).

Kwestie dotyczące pozyskiwania danych osobowych od potencjalnych pracowników przez przyszłego pracodawcę są w szczególności przedmiotem regulacji ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.). I tak, zgodnie z art. 22^1 § 1 tej ustawy, pracodawca ma prawo żądać od osoby ubiegającej się

[332] DOLiS-035-60/13
[333] DOLiS-035-155/13

o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko, 2) imiona rodziców, 3) datę urodzenia, 4) miejsce zamieszkania (adres do korespondencji), 5) wykształcenie, 6) przebieg dotychczasowego zatrudnienia. § 4 tego przepisu precyzuje, iż pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Wskazano, że należy się również odwołać się do przepisów ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. Nr 227, poz. 1505 z późn. zm.), w tym do jej art. 4, który przesądza, jaka osoba może zostać zatrudniona w służbie cywilnej, oraz do rozdziału 3 tej ustawy, zatytułowanego „Nawiązanie stosunku pracy w służbie cywilnej", które w pewnym zakresie traktują o uprawnieniach podmiotu organizującego nabór w zakresie przetwarzania danych osobowych (np. art. 28).

Konstatując stwierdzić należy, iż przeprowadzając nabór do służby cywilnej, na przetwarzanie danych osobowych, których konieczność podania wynika ze szczególnych, obowiązujących w tym sektorze przepisów prawa, nie jest potrzebna zgoda kandydata. Ponadto uwzględniając konstytucyjną zasadę legalizmu działania podmiotów publicznych (art. 7 Konstytucji RP), nie jest także dopuszczalne żądanie innych, niż wynikające z tychże (tudzież konieczne do zweryfikowania spełniania określonych ustawowo wymogów), danych osobowych.

W świetle art. 7 pkt 5 ustawy o ochronie danych osobowych, zgoda osoby, której dane dotyczą 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 i może być odwołana w każdym czasie. Jakkolwiek z definicji tej nie wynikają szczegółowe zasady formułowania zgody, niemniej jednak z treści klauzuli zgody na przetwarzanie danych osobowych powinno w sposób niebudzący wątpliwości wynikać w jakim celu, w jakim zakresie i przez kogo dane osobowe mogą być przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego na co się godzi.

W odpowiedzi odniesiono się również do kwestii okresu przechowywania dokumentów, które zawierają w swej treści dane osobowe. Z punktu widzenia przepisów o ochronie danych osobowych istotnym pozostaje, aby administrator danych kierował się w swych działaniach związanych z procesem ich przetwarzania tzw. zasadą ograniczenia czasowego, wynikającą

z treści art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych[334]. Na marginesie wskazano, że dobrą praktyką pozostaje istnienie określonej instrukcji kancelaryjnej, która w sposób precyzyjny, uwzględniając „przydatność" danych w określonym procesie, uwzględni kwestie ich usuwania (niszczenia, czy anonimizacji w rozumieniu ustawy o ochronie danych osobowych). Wartym rozważenia pozostaje być może stworzenie określonych wzorów oświadczeń (np. oświadczenia woli w przedmiocie zgody na przetwarzanie danych osobowych), ich rozpowszechnienie (np. poprzez stronę internetową) oraz wprowadzenie zasady korzystania przez kandydatów z ustalonego wzoru, celem wyeliminowania konieczności przeszukiwania nadsyłanych dokumentów pod kątem istnienia oświadczenia woli w przedmiocie zgody na przetwarzanie danych osobowych, które co najwyżej może być pozyskiwane w odniesieniu do danych nieokreślonych w powołanych wyżej przepisach Kodeksu pracy. W dalszym ciągu jednak ich pozyskiwanie winno być ograniczone zasadą adekwatności danych w stosunku do celów ich przetwarzania, obowiązującą administratora danych (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych).

W analizowanym okresie sprawozdawczym Generalny Inspektor odpowiedział również na **pytanie Ministerstwa Sprawiedliwości dotyczące kwestii, jak postąpić z listą podpisów, która jest załącznikiem do pisma stanowiącego sprzeciw wobec propozycji poprawek do projektu ustawy o zmianie ustaw regulujących wykonywanie niektórych zawodów[335].**

Odpowiedź na zapytanie wskazywała, że w sytuacji, gdy określone zagadnienia są przedmiotem regulacji innych aktów prawnych, należy w pierwszej kolejności do nich się odwołać (art. 23 ust. 1 pkt 2 oraz art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych). Należy zatem wziąć pod uwagę m.in. przepisy dotyczące zasad postępowania w zakresie prowadzenia przez właściwe organy władzy publicznej prac legislacyjnych, w tym m.in. przepisy uchwały nr 49 Rady Ministrów dnia 19 marca 2002 r. – Regulamin pracy Rady Ministrów (M.P. Nr 13, poz. 221 z późn. zm.) oraz uchwały Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r. – Regulamin Sejmu Rzeczypospolitej Polskiej (t.j. M.P. z 2012 r. poz. 32 z późn. zm.). Przepisy te odnoszą się bowiem do procedur związanych z poszczególnymi

[334] Zgodnie z ww. przepisem, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
[335] DOLiS-035-839/13

etapami prowadzonych prac legislacyjnych. Podstawy przetwarzania danych osobowych tzw. zwykłych (jak np. imię, nazwisko, adres zamieszkania, numer dowodu osobistego) przez podmioty z sektora publicznego należy bowiem upatrywać w przesłance przetwarzania danych wskazanej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Przepis ten stanowi, iż wykonywanie na danych osobowych jakichkolwiek operacji jest dopuszczalne, jeżeli jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Wobec powyższego należałoby się zastanowić nad zasadnością „odesłania" listy zawierającej dane osobowe osób „związanych ze środowiskiem rzeczoznawców majątkowych" w kontekście powstania swego rodzaju dokumentacji danego podmiotu, który – pozostając w strukturze podmiotów władzy publicznej – obowiązany jest do stosowania zarówno ww. przepisów prawa, jak i przepisów odnoszących się do konieczności odpowiedniego archiwizowania przez organy państwowe dokumentacji powstałej w związku z wykonywaniem ich zadań (np. ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach – t.j. Dz. U. z 2011 r. Nr 123, poz. 698 z późn. zm.). Z punktu widzenia przepisów o ochronie danych osobowych istotny w poruszanym aspekcie pozostaje przede wszystkim problem należytego zabezpieczenia pozyskanych danych osobowych przed dostępem do nich osób nieupoważnionych i nieudostępnianie ich innym podmiotom, jeżeli nie legitymują się właściwą podstawą prawną ku ich przetwarzaniu (art. 36 ust. 1 ustawy o ochronie danych osobowych w zw. z powoływanym już art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych).

Generalny Inspektor ustosunkowywał się również do zapytania przedstawionego przez **Zakład Ubezpieczeń Społecznych**, do którego zwróciła się jedna z uczelni wyższych z propozycją zawarcia umowy zlecenia o wygenerowanie zbioru danych jednostkowych, polegające na przetworzeniu dostarczonych przez uczelnię informacji o jego absolwentach i informacji uzyskanych z zasobów. Przekazanie **danych o zatrudnieniu absolwentów szkół wyższych** miałoby nastąpić w oparciu o umowę powierzenia danych, a miałoby służyć realizowaniu obowiązków uczelni w zakresie monitorowania karier absolwentów po ukończeniu studiów[336].

W odpowiedzi poinformowano, iż przeprowadzenie wskazanego powyżej działania zdaje się być niemożliwe z kilku powodów. W pierwszej kolejności wskazano, iż zgodnie

[336] DOLiS-035-546/13

z art. 66 ust. 1, 3 i 4 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t.j. Dz. U. z 2009 r. Nr 205, poz. 1585 z późn. zm.), ZUS jest państwową jednostką organizacyjną i posiada osobowość prawną. Działa na podstawie ww. ustawy oraz innych ustaw regulujących poszczególne zakresy jego działalności. W zakresie prowadzonej działalności, o której mowa w art. 68 – 71 ustawy, Zakładowi przysługują środki prawne właściwe organom administracji państwowej – w pewnym zakresie ZUS może więc stanowić organ władzy publicznej. Organy takie – zgodnie z art. 7 Konstytucji Rzeczypospolitej Polskiej – działają na podstawie i w granicach prawa. Po wtóre wskazano, iż nie zawsze dla identyfikacji osoby fizycznej, wymagane jest bezwzględne podanie dotyczących jej danych w zakresie obejmującym – przykładowo – imię, nazwisko i adres zamieszkania. Innymi słowy, osobę fizyczną można zidentyfikować poprzez posłużenie się informacjami, które nie tylko w sposób bezpośredni, lecz również pośredni pozwolą na ustalenie tożsamości takiej osoby[337].

Analizując dalej poruszone zagadnienie trzeba wskazać, iż zgodnie z opinią Grupy Roboczej ds. Ochrony Danych Osobowych powołanej na mocy art. 29 dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.WE.23.11.1995) – której przepisy implementowane zostały do polskiego porządku prawnego mocą ustawy o ochronie danych osobowych – można uważać osobę fizyczną za „zidentyfikowaną", jeśli w grupie osób można ją odróżnić od wszystkich pozostałych członków grupy. Osoba fizyczna jest też „możliwa do zidentyfikowania", jeżeli, mimo że nie została jeszcze zidentyfikowana, taka identyfikacja jest możliwa (opinia nr 4/2007 z dnia 20 czerwca 2007 r. w sprawie pojęcia danych osobowych).

[337] Zgodnie z treścią art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2 ustawy). Art. 6 ust. 3 ustawy o ochronie danych osobowych stanowi natomiast, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. W świetle cytowanej definicji, za dane osobowe uznaje się zatem zarówno takie informacje, które pozwalają bezpośrednio na określenie tożsamości konkretnej osoby, jak również takie, które nie pozwalają na jej natychmiastową identyfikację, są jednakże przy pewnym nakładzie kosztów, czasu lub działań wystarczające do jej ustalenia. Nie będą zaś danymi osobowymi informacje, które nie pozwalają na ustalenie tożsamości osoby, bądź też na podstawie których jej zidentyfikowanie będzie wiązało się z poniesieniem nadmiernych kosztów, czasu lub działań. Często zatem uznanie określonych informacji za dane osobowe wymagać będzie odniesienia do konkretnych okoliczności sprawy uwzględniającego specyfikę danego przypadku i jego indywidualny charakter.

Ustalenie, że w określonym przypadku mamy do czynienia z danymi osobowymi nie wymaga zatem ujawnienia tożsamości osoby w ścisłym sensie. Przykładowo można wskazać, że Europejski Trybunał Sprawiedliwości w wyroku o sygn. C-101/2001 z dnia 6 listopada 2003 r. stwierdził, iż „*odniesienie na stronie internetowej do różnych osób i ich identyfikacja poprzez nazwisko lub za pomocą innych środków, na przykład poprzez podanie ich numeru telefonu lub też informacji dotyczących ich pracy lub zainteresowań stanowi przetwarzanie danych osobowych (...) w rozumieniu (...) dyrektywy 95/46/WE”*. W takiej jak przedstawiona sytuacji – niezależnie od rozważań dotyczących prawnej możliwości wykonywania przez ZUS pozaustawowych zadań – pojawiają się liczne wątpliwości w zakresie bezwzględnego braku możliwości przypisania przetworzonych przez ZUS informacji do konkretnej osoby fizycznej przez szkołę wyższą. Po trzecie wreszcie w odpowiedzi odniesiono się do istoty umowy powierzenia przetwarzania danych osobowych. Jakkolwiek art. 31 ustawy o ochronie danych osobowych wprowadza do polskiego porządku prawnego tzw. instytucję powierzenia przetwarzania danych, to jednak wyznacza granice stosowania takich umów. Co do zasady, podmiot będący administratorem danych osobowych może powierzyć przetwarzanie danych osobowych stosownie do zasad wynikających z powołanego art. 31. Zgodnie z tym przepisem powierzenie przetwarzania danych innemu podmiotowi może nastąpić w drodze umowy zawartej na piśmie. Podmiot, któremu powierzono przetwarzanie danych może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie (nie decyduje zatem samodzielnie o celach i środkach przetwarzania powierzonych mu danych, nie może przetwarzać danych dla realizacji swoich celów/interesów). Podmiot ten jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 oraz spełnić wymagania określone w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Trzeba jednak podkreślić, że podmiot, który otrzymał powierzone dane, przetwarza je w imieniu i na rzecz administratora danych. Administrator zaś może zawierać umowy powierzenia przetwarzania danych, tylko w takich sytuacjach, kiedy sam posiada uprawnienie do wykonywania zadań w zakresie objętym powierzeniem. W przedstawionej sytuacji trudno było założyć, iż uczelnia wyższa sama, we własnym zakresie, miałby możliwość zrealizowania działania polegającego

na przetworzeniu danych absolwentów w taki sam sposób, w jaki czynność tę zrealizowałby Zakład Ubezpieczeń Społecznych, wykorzystując do tego dane osobowe zgromadzone w prowadzonych przez ten podmiot bazach danych. W tym stanie rzeczy Generalny Inspektor poddał pod rozwagę prawne możliwości wykonywania przez ZUS operacji na danych osobowych przekazanych przez uczelnię wyższą

Godnym uwagi było również zapytanie dotyczące **dopuszczalności pozyskiwania danych adresowych wraz z numerem PESEL od osób uczestniczących w akcji "Ratuj Maluchy i starsze dzieci"**[338] organizowanej przez Pełnomocnika Wniosku o Referendum Edukacyjne. W odpowiedzi wskazano, iż cel taki należy potraktować jako pozyskiwanie danych osobowych dla poparcia wniosku w sprawie referendum ogólnokrajowego i wobec tego zastosowanie powinny znaleźć przepisy szczególne w stosunku do ogólnych norm ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), a mianowicie przepisy ustawy z dnia 14 marca 2003 r. o referendum ogólnokrajowym (Dz. U. z 2003 r. Nr 57 poz. 507 z późn. zm.). Zgodnie z art. 63 ust. 1 tej ustawy, Sejm może postanowić o poddaniu określonej sprawy pod referendum z inicjatywy obywateli, którzy dla swojego wniosku uzyskają poparcie co najmniej 500.000 osób mających prawo udziału w referendum. Stosownie do ust. 3, zgłoszenia wniosku, o którym mowa w ust. 1, dokonuje na piśmie pełnomocnik. Pełnomocnikiem jest osoba wskazana w pisemnym oświadczeniu pierwszych 15 osób z wykazu, o którym mowa w ust. 4. Jak stanowi art. 63 ust. 4, do zgłoszenia wniosku załącza się wykaz obywateli popierających zgłoszenie, zawierający ich imiona, nazwiska, adresy zamieszkania, numery ewidencyjne PESEL, a także własnoręcznie złożone podpisy. Wzór wykazu ustala, w drodze uchwały, Państwowa Komisja Wyborcza.

Zapewnienie danym osobowym bezpieczeństwa było tematem zapytania skierowanego do GIODO[339] w kwestii między innymi **możliwości nadania przez administratora danych uprawnień pracownikom administracji publicznej do udzielania przez nich upoważnień, o których mowa w art. 37 ustawy o ochronie danych osobowych innym pracownikom**[340]. W odpowiedzi wskazano, że powyższe zagadnienie pozostaje

[338] DOLiS-035-1792/13
[339] DOLiS-035-2678/13
[340] Zgodnie z art. 37 ustawy o ochronie danych osobowych do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych (w świetle art. 7 pkt 4 ustawy –

kwestią wewnętrznej organizacji procesu przetwarzania danych. Należy jednak przyjąć, iż nie ma przeciwwskazań do nadania przez administratora danych określonej osobie uprawnień do nadawania upoważnień do przetwarzania danych osobowych w jego imieniu. W świetle art. 37 ustawy o ochronie danych osobowych, każda osoba przetwarzająca dane osobowe w ramach działalności administratora danych, musi legitymować się takim upoważnieniem. Wskazano również, że zgodnie z art. 268a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 2013 r. poz. 267) – organ administracji publicznej może w formie pisemnej upoważniać pracowników kierowanej jednostki organizacyjnej do załatwiania spraw w jego imieniu w ustalonym zakresie, a w szczególności do wydawania decyzji administracyjnych, postanowień i zaświadczeń. Skoro – jak zauważył Piotr Przybysz w: *Kodeks postępowania administracyjnego. Komentarz* (wyd. IV), Wydawnictwo Prawnicze LexisNexis, Warszawa 2007 – uregulowana w powołanym wyżej przepisie instytucja tzw. przedstawicielstwa administracyjnego nie prowadzi do przeniesienia kompetencji na inny niż ustawowo wyznaczony organ właściwy, a jedynie do upoważnienia pracowników organu (urzędu) do wykonywania kompetencji organu upoważniającego w zakresie przez niego ustalonym, to brak jest jakichkolwiek przeciwwskazań, by przedmiotem upoważnienia było – o ile taka jest wola administratora danych – przyznanie prawa do nadawania podległym sobie pracownikom upoważnień stosownie do art. 37 ustawy o ochronie danych.

W innej ze spraw przedstawionej przez jeden z urzędów marszałkowskich pytanie dotyczyło **procedur związanych z ochroną danych osobowych zapisanych na dysku twardym komputera w razie konieczności transportowania powyższego sprzętu**[341]. W odpowiedzi wskazano, że na administratorze danych osobowych spoczywają obowiązki określone mocą stosownych przepisów, m. in.: obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, o których mowa w art. 36 – 39 ustawy, zaś w przypadku przetwarzania danych w systemie informatycznym – w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych

jest nim organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych).

[341] DOLiS – 035-3051/13

osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). W tym miejscu wypada wskazać treść podpunktu V Załącznika A do w/w rozporządzenia (A. Środki bezpieczeństwa na poziomie podstawowym): *Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.* Wskazano również na obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Wskazany w art. 26 ust. 1 ustawy obowiązek zapewnienia, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 tego przepisu, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane; przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Dopełnienie powyższych obowiązków efektywnie wpływa również na realizację powinności zapewnienia przez administratora danych osobom, których dane dotyczą, praw do kontroli procesu przetwarzania ich danych osobowych, stosownie do przepisów rozdziału 4 ustawy o ochronie danych osobowych.

W odpowiedzi wskazano również, że dysponując stosownymi wytycznymi administrator danych samodzielnie powinien zadecydować o doborze odpowiednich środków które zapewnią ochronę w procesie przetwarzania danych osobowych, tak aby mając na uwadze zakres, kategorie danych oraz okoliczności ich przetwarzania zabezpieczyć je przed udostępnieniem osobom nieupoważnionym.

8.1.2. Banki i inne instytucje finansowe

W 2013 r. wciąż częste były pytania o **zakres danych osobowych, jakimi może dysponować bank** w przypadku zawierania określonych rodzajów umów, np. umowy lokaty, rachunku bankowego[342]. W odpowiedzi Generalny Inspektor wskazywał na właściwe przepisy prawa, m.in. przepisów ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2012 r. poz. 1376 z późn. zm.), czy ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu

[342] DOLiS-035-1604/13

praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2010 r. Nr 46, poz. 276 z późn. zm.).

Zasady prowadzenia, jak również elementy jakie powinna zawierać umowa rachunku bankowego (zgodnie z art. 49 ust. 1 pkt 3 m.in. rachunki terminowe lokat oszczędnościowych) określają przepisy Rozdziału 3 Prawa bankowego. Jak stanowi, art. 52 ust. 2 pkt 1 tej ustawy, umowa rachunku bankowego powinna określać w szczególności strony umowy. Ponadto zgodnie z art.112b Prawa bankowego, banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych. Zgodnie zaś z art. 8 ust. 1 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu instytucja obowiązana (m.in. bank) 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. Instytucja obowiązana (m.in. bank) przeprowadzająca transakcję, której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, ma obowiązek zarejestrować taką transakcję, bez względu na jej wartość i charakter (ust. 3 tego przepisu).

W zakresie **uprawnienia banków do wykonywania kopii dowodu osobistego**[343] Generalny Inspektor wskazywał, że kwestia ta jest przedmiotem szczególnych regulacji ustawowych, które znajdą tutaj bezpośrednie zastosowanie. Jeśli bowiem do przetwarzania danych osobowych w określonej dziedzinie działalności odnoszą się szczególne przepisy prawa, to stosuje się je przed przepisami o ogólnym charakterze, jakimi są przepisy ustawy o ochronie danych osobowych. Ustawa ta odsyła do właściwych przepisów szczególnych mocą art. 23 ust. 1 pkt 2 i art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

Innymi słowy z punktu widzenia przepisów ustawy o ochronie danych osobowych istotne jest, aby podmiot, który dokonuje czynności pozyskiwania danych osobowych legitymował się jedną z przesłanek legalności przetwarzania, w tym gromadzenia danych osobowych, które dla danych tzw. zwykłych (jak np. imię, nazwisko, adres zamieszkania) określone zostały w art. 23 ust. 1, zaś dla danych szczególnie chronionych - w art. 27 ust. 1 i 2, oraz aby kopiowanie dokumentów nie prowadziło do gromadzenia danych w zakresie

[343] DOLiS-035-2622/13, DOLiS-035-14/13.

szerszym, niż to jest konieczne dla realizacji celu, w jakim dane są przetwarzane (art. 26 ust 1 pkt 3).

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. Podmiotem uprawnionym z art. 112b Prawa bankowego jest bank. Zgodnie z definicją zamieszczoną w art. 2 tej ustawy, bank jest osobą prawną utworzoną zgodnie z przepisami ustaw, działającą na podstawie zezwoleń uprawniających do wykonywania czynności bankowych obciążających ryzykiem środki powierzone pod jakimkolwiek tytułem zwrotnym. 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 (art. 112b Prawa bankowego). Ustawa o ochronie danych osobowych zobowiązuje każdego administratora danych do przestrzegania zasady celowości i adekwatności, wyrażającej się w obowiązku precyzyjnego i ścisłego określenia celu przetwarzania określonego rodzaju danych, a następnie dostosowanie do tego celu zakresu przetwarzanych danych.

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

W zakresie podstaw prawnych pozyskiwania danych przez banki w opisanym przypadku warto również wskazać na art. 70 Prawa bankowego. Mocą tego przepisu, bank uzależnia przyznanie kredytu od zdolności kredytowej kredytobiorcy. Przez zdolność kredytową rozumie się zdolność do spłaty zaciągniętego kredytu wraz z odsetkami w terminach określonych w umowie. Kredytobiorca jest obowiązany przedłożyć na żądanie banku dokumenty i informacje niezbędne do dokonania oceny tej zdolności (ust. 1) i aby umożliwić podejmowanie przez bank czynności związanych z oceną sytuacji finansowej i gospodarczej oraz kontrolę wykorzystania i spłaty kredytu (ust. 2).

Z regulacji powołanego art. 70 wynika zatem obowiązek banku zbadania zdolności kredytowej podmiotu ubiegającego się o kredyt. Wskazać jednak należy, 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.

Nadal często przedmiotem wątpliwości było przekazywanie, a następnie **przetwarzanie danych osobowych przez Biuro Informacji Kredytowej S.A.** - w szczególności warunki legalizujące takie działanie uregulowane w przepisach Prawa bankowego - jak również uchybienia w zakresie aktualizacji informacji kredytowej, w tym w ogóle brak przekazywania przez banki informacji o zaistniałych zmianach lub opóźnienia w przekazywaniu takich informacji[344]. Mocą art. 105a ust. 3 ustawy z dnia z dnia 29 sierpnia 1997 r. Prawo bankowe (t. j. Dz. U. z 2002 r. Nr 7, poz. 665 z późn. zm.), banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, mogą przetwarzać informacje stanowiące tajemnicę bankową dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, a po zaistnieniu tych okoliczności upłynęło

[344] DOLiS-035-2558/13

co najmniej 30 dni od poinformowania tej osoby przez bank lub inną instytucję ustawowo upoważnioną do udzielania kredytów o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową, bez jej zgody (art. 105a ust. 3).

Powyższe warunki - legalizujące przetwarzanie danych osobowych przez banki oraz upoważnione do tego instytucje, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, bez zgody podmiotu tych danych - muszą zostać spełnione łącznie. Stanowisko takie poparł Wojewódzki Sąd Administracyjny w wyroku z dnia 30 listopada 2006 r. (sygn. II SA/Wa 1734/2006).

8.1.3. Służba zdrowia

W zakresie spraw dotyczących **ochrony zdrowia i przetwarzania danych przez podmioty lecznicze** w 2013 r. pojawiły się pytania o dopuszczalność **wykorzystywania danych pacjentów dla celów prowadzenia badań naukowych**[345]. W większości przypadków ze względu na brak znajomości wszystkich szczegółów określonego projektu badawczego wyjaśniano, że GIODO nie może w pełni ocenić dopuszczalności udostępnienia danych na te cele, jednakże wskazując przy tym na właściwe przepisy ustawy o ochronie danych osobowych odnoszące się do tych kwestii.

Zasadą ogólną jest, że dopuszczalność udostępnienia danych w określonej sytuacji uzależniona jest od spełnienia jednej z przesłanek legalności takiego działania określonych w przepisach ustawy. W odniesieniu do danych osobowych tzw. zwykłych, przesłanki legalności udostępniania (będącego formą przetwarzania) określone zostały w art. 23 ust. 1 ustawy, zaś danych szczególnie chronionych – których katalog wymienia art. 27 ust. 1 - w ust. 2 tego przepisu. W każdym konkretnym przypadku to administrator danych w oparciu o powyższe przepisy oraz przy uwzględnieniu rodzaju danych osobowych, celu oraz uzasadnienia potrzeby posiadania danych przez podmiot, który występuje o ich udostępnienie, powinien dokonać oceny w zakresie dopuszczalności takiego udostępnienia. Przy czym podkreślenia wymaga, iż to podmiot występujący o udostępnienie określonych informacji powinien wskazać podstawę prawną upoważniającą go do uzyskania danych.

[345] DOLiS-035-1075/13, DOLiS-035-1762/13, DOLiS-035-204/13

Warto również podkreślić, że zgodnie z art. 26 ust. 1 pkt 1 i 2 administrator danych zobowiązany jest do dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2. Jak stanowi ust. 2 powołanego przepisu, przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne jedynie wówczas, jeżeli nie narusza praw i wolności osób, których dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych i z zachowaniem przepisów art. 23 i 25 ustawy.

Ustawa o ochronie danych osobowych przewiduje możliwość przetwarzania w celach naukowych również danych tzw. „wrażliwych", których katalog określony został w art. 27 ust. 1, i których przetwarzanie jest co do zasady zabronione. Zgodnie z art. 27 ust. 2 pkt 9 dopuszczalność przetwarzania danych tej kategorii jest możliwa, jeśli jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego. Przy czym publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone.

Generalnego Inspektora Ochrony Danych Osobowych pytano również o zasady i podstawy prawne **zaopatrywania pacjentów w znaki identyfikacyjne**[346]**.** Stosownie do art. 36 ust. 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2013, Nr 217), pacjentów szpitala zaopatruje się w znaki identyfikacyjne. Znak identyfikacyjny, o którym mowa w ust. 3, zawiera informacje pozwalające na ustalenie imienia i nazwiska oraz daty urodzenia pacjenta, zapisanych w sposób uniemożliwiający jego identyfikację przez osoby nieuprawnione (art. 36 ust. 5 pkt 1 ww. ustawy). Rozporządzenie Ministra Zdrowia z dnia 20 września 2012 r. w sprawie warunków, sposobu i trybu zaopatrywania pacjentów szpitala w znaki identyfikacyjne oraz sposobu postępowania w razie stwierdzenia ich braku (Dz. U. 2012 r. Nr 1098), wskazuje wyłącznie, iż pacjenta zaopatruje się w znak identyfikacyjny przy przyjęciu do szpitala, po ustaleniu jego tożsamości (§ 1 pkt 1 tego rozporządzenia). Stosownie do § 3, znak identyfikacyjny umieszcza się 1) na opasce, 2) na zdjęciu – w przypadku, o którym mowa w § 5 ust. 1 – oraz w indywidualnej dokumentacji medycznej pacjenta.

[346] DOLiS-035-1326/13, DOLiS-035-897/13, DOLiS-035-351/13

Przepisy te nakładają na szpitale obowiązek zaopatrywania pacjentów w znaki identyfikacyjne poprzez stosowanie opasek (zakładanych na nadgarstek pacjenta, ewentualnie kostkę nogi) albo zdjęć pacjenta, wskazując przy tym, że znaki te mają zawierać informacje pozwalające na ustalenie tożsamości pacjenta, ale w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione. Takie brzmienie przepisów czyni po stronie szpitali dowolność przyjętego rozwiązania w tym zakresie, z zachowaniem oczywiście ww. wytycznych. Zatem do decyzji poszczególnych szpitali pozostawiono kwestię, jakie informacje będą zamieszczane na takiej opasce.

Należy również poddać pod rozwagę administratora danych, 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. Istotne zatem jest zapewnienie bezpieczeństwa tych danych przed dostępem do nich osób trzecich.

Zapytania od pacjentów dotyczyły również zakresu danych wymaganych przy **rejestracji pacjenta w placówce służby zdrowia,** np. tego, czy rejestratorka ma prawo pytać o numer PESEL[347]. W odpowiedzi poinformowano, że kwestie dotyczące świadczenia usług medycznych są przedmiotem regulacji m.in. przepisów 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.) oraz ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U. z 2013 r. poz. 217), a także wydanych na ich podstawie aktów wykonawczych. Tytułem przykładu można wskazać, iż art. 20 pierwszej z przywołanych ustaw przesądza m.in. jakiego rodzaju dane osobowe wpisywane są w poszczególnych pozycjach listy oczekujących na udzielenie świadczenia opieki zdrowotnej w szpitalach i świadczenia specjalistycznego w ambulatoryjnej opiece zdrowotnej. Zgodnie z ust. 3 tego przepisu są to – wpisywane za zgodą świadczeniobiorcy lub jego przedstawiciela ustawowego – numer kolejny, data i godzina wpisu, imię i nazwisko świadczeniobiorcy, numer PESEL, a w przypadku jego braku - numer dokumentu potwierdzającego tożsamość świadczeniobiorcy, rozpoznanie lub powód przyjęcia, adres świadczeniobiorcy, numer telefonu lub oznaczenie innego sposobu komunikacji ze świadczeniobiorcą lub jego opiekunem, termin udzielenia świadczenia, imię i nazwisko oraz podpis osoby dokonującej

[347] DOLiS-035-100/13

wpisu. W sytuacji skreślenia z listy określonej osoby – wpisywana jest także data i przyczyna skreślenia świadczeniobiorcy (pkt 4).

Podkreślić należy jednakże, iż powyższa sytuacja nie obejmuje przypadków przetwarzania danych osobowych w związku z czynnością rejestracji osoby zainteresowanej udzieleniem jej określonego „zwykłego" świadczenia opieki zdrowotnej np. w ambulatorium (przychodni, poradni, ośrodku zdrowia).

Mając powyższe na uwadze należy uwzględnić również ogólne zasady i obowiązki wynikające z ustawy o ochronie danych osobowych, m.in. wskazany w jej art. 26 ust. 1 obowiązek zapewnienia, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 tego przepisu, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. O ile zatem brak jest szczególnych przepisów prawa regulujących kwestie rejestracji w danej placówce zdrowia w tzw. „zwykłym trybie", zakres danych o osobie pozyskiwany na okoliczność umieszczenia przyszłego pacjenta na liście i przypisania mu numeru w kolejce pacjentów, winien być poprzedzony dogłębną analizą art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Niemniej jednak, dla dokładnego zidentyfikowania osoby w tym przypadku (choćby w przypadku osób o tożsamych imionach i nazwiskach) pozyskiwanie nr PESEL zdaje się być zasadne.

W 2013 r. nadal zgłaszane były Generalnemu Inspektorowi wątpliwości co do podstawowych zagadnień będących przedmiotem regulacji ustawy o ochronie danych osobowych, jak na przykład **co należy rozumieć pod pojęciem danych o stanie zdrowia**[348]**.** Generalny Inspektor wyjaśniał, że zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych 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. Podkreślenia wymagało, iż na potrzeby ustawy o ochronie

[348] DOLiS-035-208/13

danych osobowych nie zdefiniowano pojęcia „dane o stanie zdrowia". Nie wydaje się także, aby w polskim porządku prawnym istniała ustawowa, ogólna definicja tego terminu. Być może pewną wskazówką interpretacyjną mogłyby okazać się np. przepisy rozporządzenia Ministra Zdrowia z dnia 18 maja 2011 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych (Dz. U. Nr 125, poz. 712), która wymienia „części składowe" stanowiące część dokumentacji medycznej.

Niemniej jednak motyw 26 projektowanego 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) (2012/0011 (COD) – mającego zastąpić dyrektywę nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U.UE L 1995.281.31 z późn. zm.) – stanowi, że „dane osobowe dotyczące stanu zdrowia powinny w szczególności obejmować wszelkie dane dotyczące stanu zdrowia podmiotu danych, informacje na temat rejestracji osoby fizycznej w celu świadczenia usług zdrowotnych; informacje o płatnościach danej osoby fizycznej za opiekę zdrowotną lub kwalifikowaniu się danej osoby do korzystania z opieki zdrowotnej; numer, symbol lub oznaczenie przypisane danej osobie wyłącznie w celu identyfikowania jej dla potrzeb świadczenia opieki zdrowotnej; wszelkie informacje na temat tej osoby zebrane w okresie świadczenia opieki zdrowotnej na jej rzecz; informacje pochodzące z badań laboratoryjnych lub lekarskich dotyczących części ciała lub płynów ustrojowych, w tym próbek biologicznych; informacje umożliwiające identyfikację osoby świadczącej usługi opieki zdrowotnej na rzecz danego pacjenta oraz wszelkie informacje np. na temat choroby, niepełnosprawności, ryzyka choroby, historii medycznej, leczenia klinicznego lub aktualnego stanu fizjologicznego lub biomedycznego podmiotu danych, niezależnie od ich źródła, którym może być np. lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne, badanie diagnostyczne in vitro." Omówione szerokie rozumienie pojęcia dane osobowe przyjęte w projekcie wskazanego rozporządzenia wyznacza pewien kierunek myślenia o zakresie definicji tych danych sensytywnych, jakim pozostają dane o stanie zdrowia.

Generalny Inspektor wyjaśniał również, jak należy rozumieć przesłankę określoną w art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych, która stanowi jeden z wyjątków od

ogólnego zakazu przetwarzania danych osobowych natury szczególnie chronionej. Zaznaczył, że obszar stosowania upoważnienia, o którym mowa w tym przepisie, zakreślony został przez cel przetwarzania danych oraz kryterium podmiotowe. Zgodnie z jego treścią przetwarzanie tego typu danych jest dopuszczalne, jeżeli jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych. W literaturze przedmiotu wskazuje się, iż zarówno cel, jak i krąg uprawnionych podmiotów wyznaczone zostały określeniami o szerokim i elastycznym zakresie. Przez pojęcie ochrony stanu zdrowia, leczenia i świadczenia usług medycznych rozumieć należy także działania profilaktyczne, diagnostyczne, rehabilitacyjne (w tym kuracyjne). Tak więc dopuszczalne jest przetwarzanie danych o stanie zdrowia pacjenta również przez te podmioty medyczne, które np. uczestniczą w kierowaniu pacjenta na leczenie uzdrowiskowe. Z kolei osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych to „personel medyczny", który tworzą nie tylko lekarze, ale również personel pomocniczy (np. pielęgniarki, czy laboranci), tudzież rehabilitanci.

Do kręgu uprawnionych ustawa zalicza też osoby, które „zarządzają udzielaniem usług medycznych". Chodzi tu głównie o personel administracyjny zatrudniony w sektorze szeroko rozumianych usług medycznych, wykonujący rozmaite funkcje sekretarskie, funkcje związane z ewidencją pacjentów, prowadzeniem statystyki, archiwizacją dokumentów medycznych, itp. Natomiast usługi medyczne nie rozciągają się na sektor ubezpieczeń na zdrowie czy życie. Warunkiem powołania się na analizowane upoważnienie jest stworzenie pełnych gwarancji ochrony danych osobowych. Dotyczy to w pierwszym rzędzie przestrzegania tajemnicy lekarskiej i tajemnicy nałożonej przez prawo lub umowę na inne osoby pracujące w sektorze szeroko rozumianych usług medycznych. Należy przy tym uwzględniać stosowanie odpowiednich zabezpieczeń informatycznych uniemożliwiających dostęp do danych osobom nieupoważnionym[349].

Przedmiotem wątpliwości zgłoszonych GIODO w 2013 r. był również **zakres danych osobowych przekazywanych organom państwowej inspekcji sanitarnej na podstawie**

[349] zob. Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Wydanie V, Lex 2011.

zgłoszeń, o których mowa w art. 27 ust. 1 i 4 ustawy o zapobieganiu oraz zwalczaniu zakażeń u ludzi[350]**.**

W odpowiedzi wyjaśniono, że kwestie dotyczące uprawnień i obowiązków świadczeniobiorców oraz inspekcji sanitarnej w zakresie zapobiegania oraz zwalczania zakażeń i chorób zakaźnych u ludzi są przedmiotem regulacji m.in. przepisów ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. Nr 234, poz. 1570 z późn. zm.). Ustawa ta stanowi podstawę do pozyskiwania przez wskazane w jej treści organy inspekcji sanitarnej określonych informacji, po pierwsze – niejako z urzędu (w sytuacji zaistnienia okoliczności wynikających z ustawy – art. 27 – art. 29 ww. ustawy), a po wtóre – na żądanie państwowej inspekcji sanitarnej – w związku z prowadzonym postępowaniem epidemiologicznym (art. 32a). Dodać należało, iż to na administratorze danych władającym określonym zakresem informacji spoczywa obowiązek dokonania oceny, czy podmiot zwracający się o ich udostępnienie posiada ku temu odpowiednią podstawę prawną. Wobec wątpliwości w przedmiocie zasadności wniosku, administrator danych może wystąpić do podmiotu oczekującego na udzielenie informacji o wskazanie przepisu prawa będącego bezpośrednią podstawą otrzymania danych.

Podobnie jak w poprzednich latach sprawozdawczych, także w 2013 r. wiele spraw dotyczyło zastrzeżeń, co do sposobu **zabezpieczenia danych o stanie zdrowia oraz przypadków zaginięcia dokumentacji medycznej**[351]**.** W odpowiedzi GIODO wskazywał, że z 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.) oraz rozporządzenia 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), wynika określony sposób tworzenia i przechowywania dokumentacji medycznej przez podmiot udzielający świadczeń zdrowotnych. Jak stanowi art. 24 ust. 1 powołanej ustawy pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeniach zdrowotnych, a dane zawarte w dokumentacji medycznej podlegają ochronie określonej w niniejszej ustawie oraz w przepisach odrębnych (art. 23 ust. 1 i 2 cytowanej ustawy). Ponadto w celu realizacji prawa, o którym mowa w art. 23 ust. 1, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać

[350] DOLiS-035-518/13
[351] DOLiS-035-3650/13, DOLiS-035-3299/13, DOLiS-035-3576/13.

dokumentację medyczną w sposób określony w niniejszym rozdziale oraz zapewnić ochronę danych zawartych w tej dokumentacji. Z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta wynika również obowiązek poszanowania prywatności, intymności i godności pacjenta (art. 13 i 14 ustawy). Zgodnie z przepisami ustawy pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego (art. 14 tej ustawy). Wskazać również należy, że obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a 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.). Również Kodeks Etyki Lekarskiej zobowiązuje do poszanowania intymności i prywatności pacjenta.

GIODO wskazywał również, że przypadki naruszenia praw pacjentów należy zgłaszać do Rzecznika Praw Pacjenta jako organu ustanowionego w celu ochrony praw pacjenta określonych w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta oraz w przepisach odrębnych. Na gruncie ustawy o ochronie danych osobowych istotne jest właściwe dopełnienie przez administratora danych obowiązków dotyczących zabezpieczenia danych. Do obowiązków tych należy właściwe zabezpieczenie danych, co wynika w szczególności z rozdziału 5 ustawy o ochronie danych osobowych, jak i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Powyższy obowiązek spoczywa na administratorze danych, który w konkretnych warunkach i okolicznościach przetwarzania musi zapewnić danym skuteczną ochronę przed potencjalnymi zagrożeniami. Należy przy tym podkreślić, że dobór odpowiednich środków powinien uwzględniać charakter przetwarzanych danych, co oznacza, że w przypadku danych tzw. „sensytywnych", wymienionych w art. 27 ust. 1 ustawy, zastosowane środki powinny im zapewniać bardziej intensywną ochronę.

Ponadto stosownie do postanowień art. 26 ust. 1 administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Ta generalna

zasada znajduje swoje rozwinięcie w przepisach ustawy określających m.in. wymogi, jakie powinien spełnić administrator w celu zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Jednym z podstawowych obowiązków spoczywających na administratorze danych jest wynikający z art. 36 ust. 1 ustawy obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Niewywiązanie się z powyższych obowiązków może w konsekwencji prowadzić do powstania odpowiedzialności karnej na podstawie art. 51 i 52 ustawy. W myśl pierwszego ze wskazanych przepisów, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 51 ust. 2 ustawy). Zgodnie natomiast z art. 52 ustawy, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Znamieniem przestępstwa określonego w art. 52 ustawy jest samo niedopełnienie obowiązku ochrony danych osobowych, choćby dane nie zostały zabrane, zniszczone lub uszkodzone.

8.1.4. Zatrudnienie

Jedno z zapytań dotyczyło **umieszczania numeru PESEL na przepustkach upoważniających do wejścia na teren zakładu przemysłowego**[352]. W odpowiedzi poinformowano, iż numer PESEL, którego przetwarzanie przez pracodawcę co do zasady nie jest zabronione, nie jest daną służbową w znaczeniu, w jakim jego przetwarzanie byłoby niezbędne do wykonywania obowiązków służbowych. Z informacją w postaci nr PESEL należy postępować w sposób wyważony i wykorzystywać ją tylko wtedy, jeżeli inne rozwiązania organizacyjne nie będą mogły mieć zastosowania. Nie powinno dochodzić do ujawniania numeru PESEL na rzecz innych pracowników/osób związanych z działalnością

[352] DOLiS-035-2205/13

zakładu, gdy nie jest to niezbędne. W związku z tym przed umieszczeniem numeru identyfikacyjnego PESEL na przepustce należy ostrożnie wyważyć celowość i adekwatność wskazanego rozwiązania, z punktu widzenia przepisów ustawy o ochronie danych osobowych zarówno odnoszących się do adekwatności i celowości, jak również bezpieczeństwa przetwarzania danych.

Przedmiotem wątpliwości w innej sprawie[353] była **kwestia umieszczenia przez pracodawcę zdjęć pracowników w elektronicznej książce telefonicznej**. W odniesieniu do tego problemu Generalny Inspektor wskazał, iż wizerunek człowieka, jako jego dobro osobiste, chroniony jest w szczególności przepisami art. 23 i 24 ustawy Kodeks cywilny, zaś w kwestii jego naruszenia orzekają sądy cywilne w trybie wynikającym z przepisów ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. Nr 43, poz. 296 z późn. zm.). Ponadto konieczne jest też uwzględnienie regulacji szczególnych w stosunku do ustawy o ochronie danych osobowych. Stanowią je przepisy prawa pracy. Pracodawca może przetwarzać dane pracownika wyłącznie w zakresie przewidzianym przepisami prawa, jak również obowiązany jest szanować prywatność (dobra osobiste) pracownika (art. 11^1 Kodeksu pracy). Aby określić, co należy rozumieć przez dobra osobiste pracownika należy na podstawie art. 300 Kodeksu pracy odwołać się do uregulowań ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.).

Jednocześnie należy poczynić zastrzeżenie, że informacje o pracowniku, jak jego imię i nazwisko, zajmowane stanowisko, służbowy adres e-mail, czy też służbowy numer telefonu są co do zasady ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. Pracodawca jest uprawniony do dysponowania określonymi danymi osobowymi pracownika. W przedstawionej sprawie pozyskiwanie wizerunku pracownika do elektronicznej książki telefonicznej mogłoby odbywać się na podstawie przesłanki określonej w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, gdy jest niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

W innej sprawie Generalny Inspektor odniósł się do sygnalizowanych w zapytaniach wątpliwości dotyczących działalności **portali internetowych, na których znajdują się**

[353] DOLiS-035-222/13

anonimowe ogłoszenia pracodawców poszukujących pracowników[354]**.** Poszukujące zatrudnienia osoby wysyłają poprzez portal swoje dokumenty aplikacyjne (w tym CV, list motywacyjny), nie wiedząc *de facto* do kogo one trafiają. Jednocześnie w ogłoszeniu oferującym pracę zawarte jest zastrzeżenie, aby umieścić klauzulę wyrażającą zgodę na przetwarzanie danych osobowych na potrzeby procesu rekrutacyjnego. Przy wypełnianiu formularza często pojawia się komunikat (choć nie zawsze) o następującej treści: „*Informujemy, że dane osobowe zawarte w dokumentach aplikacyjnych są zbierane w celu przeprowadzenia procesów rekrutacyjnych i pozostają niejawne. W razie aplikowania na ogłoszenie bez podanej nazwy firmy, informacje na temat administratora danych (pracodawcy) zostaną Ci przekazane bezpośrednio przez pracodawcę w terminie późniejszym, niezwłocznie po otrzymaniu aplikacji przez Pracodawcę. Jeżeli nie zgadzasz się na taką procedurę, prosimy o nieprzesyłanie aplikacji na to ogłoszenie"*. Podmiot, który otrzymał dokumenty z danym osobowymi pozostaje anonimowy, nie informuje zwrotnie osoby, która wysłała dokumenty aplikacyjne, że przetwarza jej dane osobowe. Osoba, które przesłała dokumenty aplikacyjne poznaje nazwę podmiotu, który otrzymał jej dokumenty tylko w przypadku, gdy podmiot taki postanowi daną osobę zaprosić do kolejnego etapu postępowania rekrutacyjnego.

W sprawie tej Generalny Inspektor poinformował, że podstawę przetwarzania przez pracodawcę danych osobowych kandydatów do pracy stanowią przepisy prawa pracy, w tym ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 1998 r. Nr 21, poz. 94 z późn. zm.), a w szczególności jej art. 221 określający zakres danych osobowych pracownika (kandydata do pracy), jakie pracodawca może gromadzić w związku z zatrudnieniem (rekrutacją). I tak, stosownie do art. 22^1 § 1 ustawy Kodeks pracy, pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko kandydata, 2) imiona rodziców, 3) datę urodzenia, 4) miejsce zamieszkania (adres do korespondencji), 5) wykształcenie, 6) przebieg dotychczasowego zatrudnienia. Art. 22^1 § 3 ustawy Kodeks pracy stanowi, iż udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą.

Ponadto Generalny Inspektor poinformował, że każdy administrator danych obowiązany jest – w zależności od tego, czy dane zbierane są bezpośrednio od osoby, której

[354] DOLiS-035-1267/13

dotyczą, czy też z innego źródła – odpowiednio do brzmienia art. 24 lub 25 ustawy, dopełnić obowiązek informacyjny. Pracodawca, który poprzez otrzymanie CV kandydata do pracy staje się administratorem jego danych osobowych, obowiązany jest zatem ten obowiązek informacyjny wobec takiej osoby spełnić. Podkreślenia wymaga, że podczas wypełniania formularza z pośrednictwem serwisu internetowego, pojawia się komunikat, iż *„informacje na temat administratora danych (pracodawcy) zostaną Ci przekazane bezpośrednio przez pracodawcę w terminie późniejszym, niezwłocznie po otrzymaniu aplikacji przez Pracodawcę(...)”*. Jeżeli zatem pracodawca spełni wobec kandydata do pracy obowiązek informacyjny określony w art. 24 ustawy o ochronie danych osobowych, stosownie do ww. zapisu, najpóźniej w momencie otrzymania CV kandydata, to wówczas nie możemy mówić o działaniu niezgodnym z przepisami ustawy o ochronie danych osobowych. Ponadto osoba, która zamierza skorzystać z serwisu internetowego w związku z poszukiwaniem ofert pracy, powinna zapoznać się z postanowieniami regulaminu tego portalu. Powinien on wskazywać, jakie są generalne zasady korzystania z tego portalu, jakie są prawa i obowiązki usługodawcy i usługobiorcy, jakie dane osobowe usługobiorcy może usługodawca przetwarzać w związku z korzystaniem z serwisu oraz na jakiej podstawie prawnej przetwarzane są dane osobowe i kto jest ich administratorem.

Pojawiały się również pytania dotyczące **pozyskiwania danych osobowych przez społecznego inspektora pracy**[355]. Generalny Inspektor Ochrony Danych Osobowych wskazał, że zadania i organizacja społecznej inspekcji pracy oraz uprawnienia i zasady postępowania społecznych inspektorów pracy są regulowane przepisami ustawy z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy (Dz. U. z 1983 r. Nr 35 poz. 163 z późn. zm.). Art. 8 tejże ustawy, który przyznaje społecznemu inspektorowi pracy prawo żądania od kierownika zakładu pracy oraz oddziału (wydziału) i od pracowników, informacji oraz okazania dokumentów w sprawach wchodzących w zakres jego działania, stanowi jednocześnie, iż wykonywanie tych czynności następuje z zachowaniem przepisów o ochronie informacji niejawnych. Przepisy nie określają wprost do jakiego rodzaju informacji i jakich dokumentów mogą mieć dostęp społeczni inspektorzy pracy w związku z dokonywaniem swoich czynności. Wszelkie zatem działania podejmowane przez społecznych inspektorów pracy związane z żądaniem udostępnienia określonych informacji, mogą wzbudzać

[355] np. DOLiS-035-2611/13

kontrowersje i powodują, że jedynie na podstawie interpretacji przepisów zawartych w przywołanej powyżej ustawie można domniemywać o zakresie uprawnień, jak również o tym, iż udostępnienie im jakiejkolwiek informacji powinno być determinowane zakresem przeprowadzonej kontroli i nie wykraczać poza jej ramy. Dokonując rozstrzygnięcia w przedmiocie udostępnienia informacji, które stanowić mogą dane osobowe, administrator danych powinien również uwzględnić obowiązki, jakie nakładają na niego przepisy o ochronie danych osobowych, w szczególności dotyczące zabezpieczenia danych osobowych (art. 36 - 39 ustawy o ochronie danych osobowych). Naruszenie powyższych obowiązków może narazić administratora danych zarówno na odpowiedzialność administracyjną przed Generalnym Inspektorem Ochrony Danych Osobowych wynikającą z przepisów ustawy o ochronie danych osobowych, jak i karną stosownie do przepisów.

Stanowczą reakcję Generalnego Inspektora Ochrony Danych Osobowych wywołały zapytania dotyczące podstaw prawnych **przetwarzania danych biometrycznych w stosunkach pracy,** np. dla celu prowadzenia ewidencji czasu pracy[356].

W sprawach dotyczących przetwarzania danych biometrycznych[357] GIODO konsekwentnie wyrażał stanowisko, że pracodawca nie ma prawa, nawet za zgodą pracownika skanować jego linii papilarnych w celu rejestracji godzin jego przyjścia i wyjścia z zakładu pracy, co potwierdzone zostało przez orzecznictwo Naczelnego Sądu Administracyjnego, m.in. w wyroku z dnia 1 grudnia 2009 r. o sygn. akt I OSK 249/09[358].

GIODO podkreślał, że wszelkie działania ograniczające konstytucyjnie zagwarantowane prawo ochrony życia prywatnego, a także ochrony danych osobowych (art. 47 i 51 Konstytucji RP), powinny znajdować ustawową podstawę. Wymieniony przepis konstytucyjny dotyczy wszelkich przypadków, w których jednostka zobowiązana zostaje do ujawniania innym podmiotom informacji o sobie. Dane biometryczne określonej osoby, takie jak np. jej linie papilarne, obraz tęczówki oka, można uznać za dane osobowe w rozumieniu definicji zawartej w art. 6 ustawy o ochronie danych osobowych. Generalny Inspektor wskazywał na opinię Grupy Roboczej art. 29 ds. ochrony danych, przyjętą w dniu 1 sierpnia 2003 r. - Dokument Roboczy w sprawie biometrii (GT 80), w której wskazano, że *„środki*

[356] DOLiS-035-2804/13, DOLiS-035-2805/13, DOLiS-035-3624/13.
[357] np. DOLiS-035-3395/13, DOLiS-035-2563/13.
[358] Stanowisko GIODO w tej sprawie można znaleźć na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych: http://www.giodo.gov.pl/348/id_art/3358/j/pl/ .

identyfikacji biometrycznej lub ich wersja numeryczna w formie wzorca są, w większości przypadków, danymi osobowymi. (...) szybki rozwój technologii biometrycznych, jak i coraz powszechniejsze ich stosowanie w ostatnich latach wymagają uważnej analizy z punktu widzenia ochrony danych. Powszechne i niekontrolowane posługiwanie się biometrią wzbudza niepokój z punktu widzenia ochrony wolności i fundamentalnych praw człowieka. (...) Szczególne zaniepokojenie związane z danymi biometrycznymi wzbudza ryzyko zmniejszenia wrażliwości ludzi spowodowane coraz większą powszechnością używania tych danych na konsekwencje, jakie przetwarzanie ich danych może mieć w ich życiu codziennym".

Porównywanie cyfrowego odwzorowania punktów charakterystycznych palca przez rejestratory czasu pracy z zapisanymi wzorcami na karcie magnetycznej jest przetwarzaniem danych osobowych w rozumieniu art. 7 pkt 2 ustawy o ochronie danych osobowych, skoro prowadzi do identyfikacji konkretnej osoby. Należy także mieć na uwadze, że pozyskanie odcisków palców pracowników, jak również porównywanie odwzorowania punktów charakterystycznych palca przez czytniki linii papilarnych z zapisanymi na nich danymi, w celu ich identyfikacji w związku z wprowadzeniem systemu dokonującego na ich podstawie kontroli dostępu do budynku, może prowadzić do naruszenia ww. zasady adekwatności przetwarzania danych, albowiem kontrolę dostępu do budynku można osiągnąć w inny sposób, lub za pomocą innych technik, niezwiązanych z przetwarzaniem danych biometrycznych. Ponadto8 nie bez znaczenia jest, iż pozyskiwanie przedmiotowych danych może prowadzić do zbyt daleko idącej ingerencji w prywatność danej osoby.

Podobne stanowisko zaprezentowane zostało przez Grupę Roboczą Artykułu 29 ds. ochrony danych we wspomnianej opinii, w której wskazała, iż *„środki identyfikacji biometrycznej lub ich wersja numeryczna w formie wzorca są, w większości przypadków, danymi osobowymi. (...) Grupa robocza uważa, że większość systemów biometrycznych dotyczy przetwarzania danych osobowych. Konieczne jest więc rozwijanie ich z pełnym uwzględnieniem zasad ochrony danych zawartych w dyrektywie 95/46/WE, a zwłaszcza w kwestii możliwości gromadzenia danych biometrycznych bez wiedzy zainteresowanej osoby i prawie pewnego związku powiązania z tą osobą".*

Do powyższego stanowiska Grupy Roboczej odwołał się Naczelny Sąd Administracyjny w powoływanym wyżej wyroku (sygn. I OSK 249/09) stwierdzając, że *„w przyjętym przez Grupę (Grupa Robocza Artykułu 29 ds. ochrony danych osobowych) w dniu 1 sierpnia 2003 r. dokumencie roboczym w sprawie biometrii przyjęto jako niezbędną*

zasadę proporcjonalności i legalności. Oznacza to, że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności wyrażona w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników (...) jest nieproporcjonalne do zamierzonego celu ich przetwarzania". Podobne stanowisko zaprezentował Naczelny Sąd Administracyjny w wyroku z dnia 6 września 2011 r. sygn. I OSK 1476/10.

Odmiennie można by rozpatrywać pozyskiwanie danych biometrycznych celem zapewnienia bezpieczeństwa jedynie w szczególnie istotnych strefach, mających charakter newralgiczny, bądź potencjalnie zagrożonych przez niepożądane działania osób trzecich. Może mieć to szczególne uzasadnienie, gdy przebywanie większości osób w innych częściach np. budynku, czy kompleksu budynków nie byłoby uwarunkowane pozyskiwaniem i przetwarzaniem danych osobowych o charakterze biometrycznym, a pozyskiwanie danych biometrycznych miałoby na celu znaczące ograniczenie dostępu do wyznaczonych stref/pomieszczeń. W takich sytuacjach systemy bezpieczeństwa wykorzystujące czytniki linii papilarnych mogą być adekwatne i uzasadnione, o ile ich stosowanie nie ma na celu kontrolowania danego pracownika, tylko służy właśnie ograniczeniu dostępu na rzecz określonego, wąskiego grona osób do budynków, czy pomieszczeń szczególnie chronionych.

8.1.5. Związki zawodowe

Jako przykład wątpliwości w zakresie przetwarzania danych osobowych w obszarze działalności **związków zawodowych**, wskazać można pytanie dotyczące **dopuszczalności udostępnienia przez pracodawcę informacji na temat imienia, nazwiska i wysokości kwoty przyznanej podwyżki płac, czy nagrody rektorskiej dla pracownika**[359]**.**

W odpowiedzi wskazano na ogólną zasadę, zgodnie z którą administrator danych analizując indywidualnie wszelkie okoliczności związane z udostępnieniem danych oraz badając, czy zachodzą przesłanki ich udostępnienia, powinien w każdym przypadku samodzielnie zdecydować w przedmiocie udostępnienia bądź odmowy ich udostępnienia,

[359] DOLiS-035-1378/13

biorąc pod uwagę obowiązujące przepisy prawa oraz ponosząc odpowiedzialność za podjęte działania, w tym zaniechanie. W przedstawionej sytuacji należy odwołać się do przepisów ustawy z dnia 23 maja 1991 r. o związkach zawodowych (t.j. Dz. U. z 2001 r. Nr 79, poz. 854 z późn. zm.) regulujących zasady prowadzenia działalności związkowej, w tym również uprawnienia i obowiązki związku zawodowego.

Prawo związków zawodowych do uzyskania określonych informacji oraz obowiązki pracodawcy reguluje przede wszystkim art. 28 ustawy o związkach zawodowych. Przepis ten stanowi, iż „pracodawca jest obowiązany udzielić na żądanie związku zawodowego informacji niezbędnych do prowadzenia działalności związkowej, w szczególności informacji dotyczących warunków pracy i zasad wynagradzania". Zgodnie natomiast z art. 27 ust. 3, regulaminy nagród i premiowania są ustalane i zmieniane w uzgodnieniu z zakładową organizacją związkową. Dotyczy to również zasad podziału środków na wynagrodzenia dla pracowników zatrudnionych w państwowej jednostce sfery budżetowej. Powołany akt prawny nie precyzuje, jakiego rodzaju informacje są niezbędne do prowadzenia działalności związkowej. Uznać zatem należy, iż zakres i rodzaj tych informacji determinowany jest zakresem ustawowych zadań związków zawodowych. Stwierdzenie, że pracodawca jest obowiązany udzielić związkowi zawodowemu informacji dotyczących zasad wynagradzania oznacza, iż ma on obowiązek udzielić związkowi informacji o wysokości funduszu płac i jego strukturze, przesłankach i wysokości kształtowania wynagrodzenia ogółu pracowników lub określonej grupy zawodowej, itp.[360] Analogiczne uwagi odnieść należy do zawartych w regulaminach nagród i premiowania zasad przyznawania nagród oraz zasad podziału środków na wynagrodzenia pracowników. W świetle powyższego wydaje się, że udostępnienie związkom zawodowym informacji dotyczących konkretnego nagrodzonego pracownika i wysokości przyznanej nagrody, nie znajduje uzasadnienia w powyższej regulacji.

Ponadto, istnieją informacje, do których dostęp możliwy jest wyłącznie za zgodą osoby, której informacje te dotyczą lub wówczas, gdy szczególny przepis prawa wprost upoważnia określone podmioty do ich uzyskania. Do tego rodzaju informacji zaliczyć należy np. informacje o wynagrodzeniu, w tym nagrodach pracownika, które – co do zasady – powinny pozostawać w gestii pracodawcy. W uchwale z dnia 16 lipca 1993 r. (sygn. akt I PZP 28/93)

[360] Zob. Zbigniew Salwa, Prawo pracy, Warszawa 1997 – 2005 Wydawnictwo Prawnicze LexisNexis.

Sąd Najwyższy orzekł, iż *„(...) uprawnienie do kontrolowania przez związki zawodowe przestrzegania prawa pracy (...) nie oznacza (...) uprawnienia do żądania od pracodawcy udzielenia informacji o wysokości wynagrodzenia pracownika bez jego zgody*", zaś *„ujawnienie przez pracodawcę bez zgody pracownika wysokości jego wynagrodzenia za pracę może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 Kodeksu cywilnego"*. Rozważając kwestię wynagrodzenia zindywidualizowanego, to należy odnieść się także do zasad ogólnych i wskazać na ugruntowane w judykaturze stanowisko, iż informacje o wynagrodzeniu pracownika, jako należące do kategorii dóbr osobistych, chronione są przepisami ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.). W uchwale z dnia 16 lipca 1993 r. (sygn. I PZP 28/93) Sąd Najwyższy orzekł, iż *„(...) ujawnienie przez pracodawcę bez zgody pracownika wysokości jego wynagrodzenia za pracę może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 kodeksu cywilnego"*. Z kolei w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 2 listopada 2005 r. (sygn. Akt VI S.A./Wa 1080/2005) stanowi się, iż „*zgodnie z art. 51 ust. 1 Konstytucji RP nikt nie może być obowiązany inaczej, niż na podstawie ustawy, do ujawniania informacji dotyczących jego osoby. (...) Prawo do wynagrodzenia może być dobrem osobistym, które co do zasady zgodnie z przepisem art. 24 Kodeksu cywilnego pozostaje pod ochroną prawa cywilnego (...)"*. Powyższe odnosi się jedynie do wynagrodzenia pracownika wypłacanego na podstawie umowy o pracę. W odniesieniu do danych osobowych stron umów cywilnoprawnych, zastosowanie znajdą ww. przepisy ustawy o ochronie danych osobowych.

Stosownie natomiast do art. 151 ust. 3 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2005 r. Nr 164, poz. 1365 z późn. zm.), w uczelni publicznej wynagrodzenia rektorów, prorektorów, kanclerzy i kwestorów są jawne, nie podlegają ochronie danych osobowych.

W innej sprawie związki zawodowe przedstawiały Generalnemu Inspektorowi wątpliwości związane z **ujawnianiem imion i nazwisk pracowników np. na drzwiach pokoi pracowniczych, na stronie internetowej pracodawcy, czy też na kaskach ochronnych**[361]. W odpowiedzi poinformowano, że z punktu widzenia zasad przetwarzania danych osobowych wynikających z przepisów ustawy nie sposób uznać za bezprawne

[361] DOLiS–035–2460/13, DOLiS–035–2414/13.

umieszczenie imienia i nazwiska, czy to na kasku czy też np. na drzwiach pokoju pracownika, a nawet na stronie internetowej pracodawcy, gdy ma to związek z pełnieniem obowiązków służbowych przez pracownika. Dane takie, jak imię i nazwisko są podstawowymi danymi służącymi do identyfikacji danej osoby. Stanowisko takie zaprezentował także w swoim orzecznictwie Sąd Najwyższy. W uzasadnieniu wyroku z dnia 19 listopada 2003 r. (sygn. I PK 590/02) Sąd stwierdził, iż *„(...) nazwisko (i imię) jest z natury rzeczy skierowanym na zewnątrz znakiem rozpoznawczym osoby fizycznej i wymienienie go (ujawnienie) przez inny podmiot w celu identyfikacji danej osoby nie może być zasadniczo uznane za bezprawne, o ile ze względu na okoliczności towarzyszące nie łączy się to z naruszeniem innego jej dobra, np. czci, godności osobistej lub prywatności”*. W tym samym wyroku można przeczytać w innym miejscu: *„najistotniejszym składnikiem zakładu pracy (przedsiębiorstwa) są ludzie, a funkcjonowanie zakładu wiąże się nierozłącznie z kontaktami zewnętrznymi - z kontrahentami, klientami (...). Dlatego pracodawca nie może być pozbawiony możliwości ujawniania nazwisk pracowników, zajmujących określone stanowiska w ramach instytucji. Przeciwne stanowisko prowadziłoby do sparaliżowania lub poważnego ograniczenia możliwości działania pracodawcy, bez żadnego rozsądnego uzasadnienia w ochronie interesów i praw pracownika (...)”*. A zatem, o ile dane o pracownikach udostępnione przez pracodawcę są ściśle powiązane z ich życiem zawodowym, a nie dotyczą prywatnej sfery ich życia, o tyle miejsce i forma ich udostępnienia (np. w intranecie czy na identyfikatorze) nie ma znaczenia.

Warto nadmienić, że wątpliwości związane z ujawnianiem imion i nazwisk pracowników w zakładach pracy przedstawiają również inne podmioty[362], w tym pracodawcy. GIODO informował, że co do zasady można ujawniać takie dane pracownika, jak imię i nazwisko czy stanowisko pracy, gdy jest to związane z pełnieniem obowiązków służbowych (dopuszczalne jest to w systemie obiegu dokumentów, w celu oznaczania odzieży ochronnej itp.).

[362] DOLiS-035-2691/13, DOLiS–035–2946/13.

8.1.6. Mieszkalnictwo

W omawianym okresie sprawozdawczym wiele zapytań związanych było z zarządzaniem nieruchomościami, w tym lokalami komunalnymi, wspólnotami mieszkaniowymi czy administrowaniem spółdzielnią mieszkaniową.

Przedmiotem wątpliwości było na przykład, czy **spółdzielnia mieszkaniowa – w przypadku zalania mieszkania wodą - jest zobowiązania do udzielenia informacji na temat właściciela mieszkania, znajdującego się nad mieszkaniem poszkodowanego**[363]. W odpowiedzi wskazano na art. 25 ust. 1 ustawy z dnia 22 maja 2003 r. o działalności ubezpieczeniowej (Dz. U. z 2010 r. Nr 11 poz. 66), zgodnie z którym sądy, prokuratura, Policja oraz inne organy i instytucje, na wniosek zakładu ubezpieczeń, w zakresie zadań przez ten zakład ubezpieczeń wykonywanych i w celu ich wykonania, w związku z wypadkiem lub zdarzeniem będącym podstawą ustalania odpowiedzialności, udzielają informacji o stanie sprawy oraz udostępniają zebrane materiały, jeżeli są one niezbędne do ustalenia okoliczności tych wypadków i zdarzeń losowych oraz wysokości odszkodowania lub świadczenia.

Kolejne pytanie dotyczyło tego, czy, czy **w świetle ustawy o ochronie danych osobowych zarządcy nieruchomości posiadają uprawnienie, aby np. wywiesić na tablicy ogłoszeń danego budynku mieszkalnego informację o liczbie osób zamieszkujących dany lokal mieszkalny**[364].

W odpowiedzi wskazano, że powyższe informacje należy traktować jak dane osobowe w rozumieniu ustawy i stosować wszystkie określone przepisami prawa zasady dotyczące ich przetwarzania. Ponadto wskazano, że tryb i zasady prowadzenia zadań gminy w zakresie utrzymania czystości i porządku w gminach określone są przepisami ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2012 r. poz. 391 z późn. zm.). Z kolei przepisy innych ustaw w przedmiotowej sprawie dotyczących zasad funkcjonowania w szczególności spółdzielni mieszkaniowych i wspólnot, tj. ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. 2003 r. Nr 119, poz. 116 z późn. zm.) i ustawy dnia 24 czerwca 1994 r. o własności lokali (Dz. U. 2003 r. Nr 188, poz. 1848 z późn. zm.), stanowić będą podstawę prawną przetwarzania danych osobowych członków spółdzielni i wspólnot. To te akty prawne określają standardy obrotu informacjami

[363] DOLiS-035-2982/13
[364] DOLiS-035-2269/13

w przedmiotowym zakresie i w żadnym z tych aktów prawnych nie ma mowy o publikowaniu informacji dotyczących członków, jako modelu dyscyplinowania ich do podawania prawdziwych danych w związku z realizacją przepisów ustawy o utrzymaniu czystości i porządku w gminach. W związku z powyższym trudno jest znaleźć konieczne podstawy prawne powyższych działań zwłaszcza, iż powyżej wskazane akty prawne stanowią także o zasadach partycypacji członków tych społeczności we wspólnych zobowiązaniach, czy o sytuacjach, dla których wewnętrzna jawność poczynań tak zarządów, czy informacji dotyczących poszczególnych osób fizycznych jest dopuszczalna.

Jedynie więc wyjątkowo i z zachowaniem szczególnej ostrożności można by przyjąć za uzasadnione rozwiązania, w których przedmiotowe informacje mogłyby być udostępnione wyłącznie członkom spółdzielni i wspólnot w ramach zgodnej z przepisami prawa kontroli zobowiązań spoczywających na spółdzielni, czy wspólnocie (w przypadku spółdzielni i wspólnot określone są tryby udostępnienia informacji i krąg odbiorców w przypadkach wyróżnionych przepisami ustawy o spółdzielniach mieszkaniowych i ustawy o własności lokali), i w związku z przyjęciem określonej właśnie metody naliczenia opłaty przez gminę. Nie będzie to jednak praktyka uzasadniona w aspekcie upublicznienia informacji (w znaczeniu podania do wiadomości bliżej nieokreślonemu kręgowi odbiorców poza członkami spółdzielni czy wspólnot) – do czego brak jest podstaw prawnych.

Wiele zapytań dotyczyło również kwestii upublicznienia informacji **na temat zaległości we wnoszeniu opłat należnych wspólnocie**[365]**.** Tak jak w poprzednich latach swojej działalności Generalny Inspektor odpowiadał, że wspólnoty mieszkaniowe są tworzone na podstawie przepisów ustawy o własności lokali, a w zakresie w niej nieuregulowanym zastosowanie znajdują przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16, poz. 93 z późn. zm.). Zgodnie z jego art. 200 każdy ze współwłaścicieli jest obowiązany do współdziałania w zarządzie rzeczą wspólną. Z powyższego wynika zatem, iż członkowie wspólnoty mieszkaniowej uprawnieni są do pozyskania danych osobowych pozostałych członków wspólnoty do celu jakim jest zarząd rzeczą wspólną i jedynie w zakresie niezbędnym do tego celu.

Zgodnie z art. 16 ust. 1 ustawy o własności lokali, jeżeli właściciel lokalu zalega długotrwale z zapłatą należnych od niego opłat lub wykracza w sposób rażący lub uporczywy

[365] Np. DOLiS-035-1513/13

przeciwko obowiązującemu porządkowi domowemu, albo przez swoje niewłaściwe zachowanie czyni korzystanie z innych lokali lub nieruchomości wspólnej uciążliwym, wspólnota mieszkaniowa może w trybie procesu żądać sprzedaży lokalu w drodze licytacji na podstawie przepisów Kodeksu postępowania cywilnego o egzekucji z nieruchomości. Aby wspólnota mogła skorzystać z tego uprawnienia, jej członkowie powinni znać dane osobowe właściciela i wysokość jego zadłużenia wobec wspólnoty.

Dopuszczalność udostępnienia członkom wspólnoty mieszkaniowej danych i informacji dotyczących zaległości we wnoszeniu opłat należnych wspólnocie przez innych jej członków, wynika z przepisów prawa, a tym samym znajduje oparcie w przesłance określonej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, zgodnie z którym przetwarzanie danych osobowych jest dopuszczalne gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Podkreślenia wymaga fakt, iż zakres danych i informacji udostępnianych innym współwłaścicielom powinien być adekwatny do ich potrzeb związanych ze zgodnym z prawem celem udostępnienia. Ponadto istotnym jest, że informacje o posiadaniu zaległości we wnoszeniu opłat należnych wspólnocie przez danego członka wspólnoty mogą być udostępnianie wyłącznie pozostałym członkom tej wspólnoty, nie jest natomiast dopuszczalnym udostępnianie tych danych osobom trzecim.

Czy **zbiór danych użytkowników osiedlowego parkingu** zawierający imiona, nazwiska i numery rejestracyjne pojazdów **podlega zwolnieniu z obowiązku rejestracji w rejestrze prowadzonym przez GIODO**[366] było kolejnym pytaniem odnoszącym się do analizowanego sektora.

Stosownie do przepisu art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), administrator danych (którym – jak wynika z art. 7 pkt 4 tej ustawy - jest organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych) jest obowiązany zgłosić zbiór danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, chyba że zachodzi jedna z przesłanek określonych w art. 43 ust. 1 ustawy, zwalniających z tego obowiązku. Wyjątków tych nie można interpretować rozszerzająco. Ponadto zwolnienie zbioru z rejestracji jest możliwe

[366] DOLiS-035-1974/13

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. Odnosząc się do art. 43 ust. 1 pkt 11 ustawy o ochronie danych osobowych wskazać należy, że przesłanka ta ma zastosowanie wobec zbioru danych „przetwarzanych w zakresie drobnych bieżących spraw życia codziennego". Ustawa o ochronie danych osobowych nie definiuje wprost wskazanego w tym przepisie pojęcia „drobne bieżące sprawy życia codziennego", niemniej jednak należy uznać, że oznacza ono sprawy drugorzędne, nie mające zasadniczego znaczenia dla administratora danych. Jeżeli zatem zbiór miałby być zwolniony z rejestracji na tej podstawie prawnej to musi on mieć charakter pomocniczy, a co za tym idzie dane w nim zawarte traktować należy jako przetwarzane w zakresie drobnych, bieżących spraw życia codziennego. Jeżeli zbiór danych użytkowników parkingu będzie zbiorem służącym do wydania identyfikatorów i do administrowania tym parkingiem, a zatem zbiorem podstawowym, a nie pomocniczym, wątpliwym jest, iż taki zbiór danych mógłby korzystać ze zwolnienia na podstawie przesłanki z art. 43 ust. 1 pkt 11 ustawy. Natomiast dane zebrane w zbiorze księgi przepustek, są traktowane jako dane przetwarzane w zakresie drobnych bieżących spraw życia codziennego, jeżeli będą to przepustki jednorazowe. Wydawanie takich przepustek służy jedynie do zapewnienia jednorazowego wejścia do budynku, a nie do stałego wstępu do budynku, czy do długotrwałego korzystania z konkretnego miejsca postojowego na parkingu, które dodatkowo jest przypisane do konkretnej osoby, dodatkowo często za odpowiednią opłatą.

W 2013 r. w dalszym ciągu wiele wątpliwości budziła kwestia zasad i warunków **instalowania na osiedlach mieszkaniowych systemów monitoringu**[367]**.** Wątpliwości te były zapewne spowodowane tym, że w polskim systemie prawa, brak jest aktu rangi ustawy kompleksowo normującego kwestie stosowania wideomonitoringu. Nie istnieje więc np. prawny wymóg tworzenia specjalnego regulaminu w związku z założeniem systemu wideomonitoringu. Ustawa o ochronie danych osobowych - analogicznie do ustawodawstwa krajowego z tego zakresu obowiązującego w większości państw członkowskich Unii Europejskiej - nie reguluje w sposób szczególny kwestii przetwarzania danych wizualnych

[367] Np. DOLiS-035-267/13, DOLiS-035-2688/13, DOLiS-035-4663/13, DOLiS-035-4666/13.

i dźwiękowych. Przy czym – co podkreśla GIODO w odpowiedziach dotyczących tego tematu - nie można *a priori* przyjmować, że korzystanie przez określony podmiot z monitoringu musi wiązać się przetwarzaniem danych osobowych w zbiorze danych w rozumieniu art. 7 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926 z późn. zm.). Nie w każdej sytuacji również wskutek monitoringu dochodzi do pozyskiwania danych osobowych w rozumieniu art. 6 ustawy o ochronie danych osobowych. W każdym przypadku konieczne jest dokonanie starannej i zindywidualizowanej oceny, czy ustawa o ochronie danych osobowych w ogóle znajduje zastosowanie. Konieczne jest przy tym uwzględnienie wyników analizy zastosowanego systemu monitoringu i jego ewentualnego powiązania z innymi systemami wykorzystywanymi przez administratora danych. W celu przekazania wskazówek w zakresie postępowania z systemami monitoringu GIODO informował, że do kwestii przetwarzania danych dźwiękowych i wizyjnych odnosi się dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (95/46/WE), stanowiąc w punkcie 14 preambuły, że „*jeżeli w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych”*. Z punktu 16 tejże preambuły wynika, iż „*przetwarzanie danych dźwiękowych i obrazowych, np. w przypadku nadzoru kamer wideo, nie wchodzi w zakres niniejszej dyrektywy, jeśli dokonywane jest dla potrzeb bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego lub też w trakcie działań organów państwowych w dziedzinie prawa karnego lub innych działań niewchodzących w zakres prawa Wspólnoty”*. Oznacza to, że rejestrowanie obrazu i dźwięku objęte jest zakresem przedmiotowym i podmiotowym dyrektywy poza wymienionymi powyżej przypadkami.

Istotne znaczenie ma w tej materii – jak dalej traktuje ww. opinia – realizacja obowiązku informacyjnego wobec osób, których dane pozyskane zostały za pomocą monitoringu, zgodnie z wymogami art. 10 i 11 ww. dyrektywy 95/46/WE. Wskazano przy tym, iż osoby te muszą mieć świadomość faktu prowadzenia wobec nich czynności nadzoru wideo. Odpowiednie tablice informacyjne o prowadzonym monitoringu powinny być widoczne, syntetyczne i umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Muszą także wskazywać cele działań nadzoru, jak również

administratora przetwarzania, a wymiary tablic muszą być proporcjonalne do miejsca, gdzie są umieszczone. Jak już wspomniano nie w każdej sytuacji wskutek monitoringu dochodzi do pozyskiwania danych osobowych w rozumieniu art. 6 ustawy. Jeżeli jednak dojdzie w konkretnej sytuacji do przetwarzania danych osobowych, wówczas zastosowanie znajdą przepisy ustawy o ochronie danych osobowych. Podkreślenia wymaga, że monitoring powinien pozostawać w zgodzie z obowiązującymi przepisami prawa odnoszącymi się chociażby pośrednio do tej kwestii.

8.1.7. Internet

W omawianym okresie sprawozdawczym, tak jak w poprzednich latach, wiele pytań dotyczyło szeroko rozumianego przetwarzania danych osobowych w Internecie.

Pytano między innymi o możliwość **pozyskiwania danych osobowych autorów wpisów na forum internetowym celem ochrony własnych dóbr osobistych**[368]. Generalny Inspektor wskazywał, że w świetle przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych dopuszczalność udostępnienia danych w określonej sytuacji zależy od kategorii danych oraz od tego, jakiemu podmiotowi i w jakim celu dane mają być udostępnione. Art. 23 ust. 1 pkt 5 ustawy stanowi, że przetwarzane danych jest dopuszczalne, jeśli 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. Za prawnie usprawiedliwiony cel, zgodnie z ustępem 4 uważa się w szczególności m.in. dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej (może tu chodzić także o dochodzenie innych roszczeń, gdyż katalog zawarty w tym przepisie jest katalogiem otwartym). Osoba zainteresowana pozyskaniem takich danych w pierwszej kolejności powinna zwrócić się do administratora tych danych o ich udostępnienie. Działanie bądź zaniechanie administratora pozostające w sprzeczności z jego obowiązkami wynikającymi z przepisów ustawy o ochronie danych osobowych można w drodze stosownego postępowania weryfikować przed Generalnym Inspektorem Ochrony Danych Osobowych. Postępowanie takie powinna inicjować skarga osoby wnioskującej o udostępnienie danych osobowych.

[368] DOLiS-035-2373/13 DOLiS-035-2373/13, DOLiS-035-3355/13, DOLiS-035-3367/13, DOLiS-035-3587/13, DOLiS-035-3668/13, DOLiS-035-3519/13, DOLiS-035-3566/13.

Niezwykle liczne były zapytania dotyczące **niezamówionej informacji handlowej** (spamu)[369]. Odpowiadając na tego rodzaju wątpliwości, w tym kierowane jedynie do wiadomości GIODO, organ ochrony danych osobowych informował, że w przypadku otrzymywania niezamówionych informacji handlowych, możliwe jest działanie w oparciu o dwa różne reżimy prawne: ustawę z dn. 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.), albo ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.)

W oparciu o przepisy szczególne ustawy o świadczeniu usług drogą elektroniczną, która reguluje kwestie dotyczące obowiązków usługodawców, związane ze świadczeniem usług drogą elektroniczną oraz zasady ochrony danych osobowych użytkowników poczty elektronicznej, zakazane jest - zgodnie z art. 10 ust. 1 - przesyłanie za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej, niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną. Informację handlową, w myśl art. 10 w/w ust. 2 ustawy, uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na jej otrzymywanie, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny. Art. 4 ust. 1 powołanej ustawy stanowi zaś, iż jeżeli ustawa wymaga uzyskania zgody usługobiorcy, to zgoda ta nie może być domniemana lub dorozumiana, a ponadto może być odwołana w każdym czasie. W myśl z art. 10 ust. 3 w/w ustawy przesyłanie niezamówionej informacji handlowej stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.). Warto w tym miejscu mieć na uwadze stanowisko Naczelnego Sądu Administracyjnego zawarte w wyroku z dnia 31 stycznia 2012 r. (sygn. akt I OSK 1317/11): *„Klauzula zgody na przetwarzanie danych osobowych w celach marketingowych powinna być sformułowana w sposób oddzielny od klauzuli zgody na otrzymywanie informacji handlowych za pomocą poczty elektronicznej”*. Zgodnie natomiast z brzemieniem art. 24 ustawy o świadczeniu usług drogą elektroniczną, przesyłanie za pomocą środków komunikacji elektronicznej niezamówionych informacji handlowych stanowi wykroczenie ścigane na wniosek pokrzywdzonego. Orzekanie w powyższych sprawach następuje w trybie przepisów o postępowaniu w sprawach o wykroczenia, zgodnie

[369] DOLiS–035-2198/13, DOLiS–035-2580/13, DOLiS–035-2594/13, DOLiS–035-2560/13, DOLiS–035-2624/13, DOLiS-035-2980/13, DOLiS–035-3691/13, DOLiS–035-3703/13.

z przepisami ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2013 r. poz. 395). Oskarżycielem publicznym zgodnie z treścią art. 17 § 1 ww. kodeksu, we wszystkich sprawach o wykroczenia, jest Policja, chyba że ustawa stanowi inaczej. Niezależnie od powyższego można także skorzystać z cywilnoprawnych środków ochrony przed niezamówioną informacją handlową: na podstawie art. 12 w zw. z art. 9 pkt 3 ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym – ochrona konsumentów przed agresywną praktyką rynkową, bądź też art. 23 i 24 Kodeksu cywilnego – ochrona dóbr osobistych (prawo do prywatności). W przypadku powództwa cywilnego właściwe pozostają sądy powszechne.

Z kolei na gruncie ustawy o ochronie danych osobowych prawa osoby, której dane dotyczą uregulowane są w rozdziale 4 ustawy o ochronie danych osobowych. Na wstępie warto zaznaczyć, że przetwarzanie tzw. zwykłych danych osobowych (takich jak np. imię i nazwisko, numer telefonu, czy adres e-mail) dopuszczalne jest tylko wtedy, gdy spełniona jest któraś z przesłanek z art. 23 ustęp 1 przywołanej ustawy, np. osoba, której dane dotyczą wyrazi na to zgodę, czy też jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przy czym za prawnie usprawiedliwiony cel uważa się w szczególności także marketing bezpośredni własnych produktów lub usług administratora danych (art. 23 ust. 4 pkt 1).

Niemniej jednak z przetwarzaniem danych na podstawie art. 23 ust. 1 pkt 5 ściśle wiąże się uprawnienie z art. 32 ust. 1 pkt 8, zgodnie z którym każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych. W razie wniesienia sprzeciwu, o którym mowa wyżej, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem. (art. 32 ust. 3 ustawy). W razie nieuwzględnienia sprzeciwu przez administratora danych możliwe jest wniesienie skargi do Generalnego Inspektora Ochrony Danych Osobowych.

W odpowiedzi na pytanie odnośnie **przechowywania informacji w postaci plików cookies**[370] GIODO wyjaśniał, że kwestia dotycząca plików cookies uregulowana została w przepisach ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.). Zgodnie z art. 173 ust. 1 Prawa telekomunikacyjnego przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego jest dozwolone, pod warunkiem że: 1) abonent lub użytkownik końcowy zostanie uprzednio bezpośrednio poinformowany w sposób jednoznaczny, łatwy i zrozumiały, o: a) celu przechowywania i uzyskiwania dostępu do tej informacji, b) możliwości określenia przez niego warunków przechowywania lub uzyskiwania dostępu do tej informacji za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi; 2) abonent lub użytkownik końcowy, po otrzymaniu informacji, o których mowa w pkt 1, wyrazi na to zgodę; 3) przechowywana informacja lub uzyskiwanie do niej dostępu nie powoduje zmian konfiguracyjnych w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego i oprogramowaniu zainstalowanym w tym urządzeniu.

Stosownie do treści ust. 2 ww. przepisu, abonent lub użytkownik końcowy może wyrazić zgodę, o której mowa w ust. 1 pkt 2, za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi. Warunków, o których mowa w ust. 1, nie stosuje się, jeżeli przechowywanie lub uzyskanie dostępu do informacji, o której mowa w ust. 1, jest konieczne do wykonania transmisji komunikatu za pośrednictwem publicznej sieci telekomunikacyjnej lub dostarczania usługi telekomunikacyjnej lub usługi świadczonej drogą elektroniczną, żądanej przez abonenta lub użytkownika końcowego (art. 173 ust. 3 Prawa telekomunikacyjnego). Zgodnie z brzmieniem ust. 4 ww. przepisu, podmioty świadczące usługi telekomunikacyjne lub usługi drogą elektroniczną mogą instalować oprogramowanie w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego przeznaczonym do korzystania z tych usług lub korzystać z tego oprogramowania, pod warunkiem że abonent lub użytkownik końcowy: 1) przed instalacją oprogramowania zostanie poinformowany bezpośrednio, w sposób jednoznaczny, łatwy i zrozumiały, o celu,

[370] DOLIS-035-1447/13

w jakim zostanie zainstalowane oprogramowanie, oraz sposobach korzystania przez podmiot świadczący usługi z tego oprogramowania; 2) zostanie poinformowany bezpośrednio, w sposób jednoznaczny, łatwy i zrozumiały, o sposobie usunięcia oprogramowania z telekomunikacyjnego urządzenia końcowego użytkownika lub abonenta; 3) przed instalacją oprogramowania wyrazi zgodę na jego instalację i używanie. Przechowywanie informacji na urządzeniu końcowym użytkownika, co odnosi się również do plików cookies, powinno odbywać się zgodnie z ww. przepisami. Istnieje obowiązek informowania abonenta lub użytkownika końcowego m.in. o celach przechowywania danych oraz w szczególności o możliwości określenia przez abonenta lub użytkownika końcowego warunków przetwarzania danych za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego urządzeniu końcowym lub za pomocą konfiguracji samej usługi. Brzmienie art. 173 Prawa telekomunikacyjnego wskazuje, że abonent lub użytkownik końcowy ma możliwość wyrażenia zgody za pomocą ustawień oprogramowania zainstalowanego w urządzeniu końcowym lub konfiguracji usługi. Przekazanie informacji oraz uzyskanie zgody, o których mowa w ust. 1, powinno nastąpić przed wprowadzeniem i rozpoczęciem przetwarzania danych.

Jedno z przykładowych pytań dotyczyło **przetwarzania danych w bazie WHOIS**[371]. Baza WHOIS jest powszechnie dostępną bazą danych o abonentach domen internetowych/podmiotach rejestrujących domeny internetowe. Głównym celem prowadzenia takiej bazy jest zapewnienie poszanowania praw użytkowników Internetu, właścicieli znaków towarowych, praw autorskich i innych dóbr chronionych prawem. Zakres danych abonenta powszechnie dostępnych w bazie WHOIS obejmuje imię i nazwisko, adres pocztowy, miasto, adres poczty elektronicznej oraz numer telefonu. Przesłanką przetwarzania danych w takim zbiorze, o ile brak jest możliwości spełnienia jednego z warunków ustanowionych mocą art. 23 ust. 1 pkt 2-5 ustawy o ochronie danych osobowych, jest zgoda osoby, której dane dotyczą. GIODO poinformował ponadto, że krajowe podmioty pośredniczące w procesie rejestracji nazw domen internetowych przyznawanych abonentom indywidualnym, działają w oparciu o porozumienia zawierane pomiędzy rejestratorem a ICANN (ang. Internet Corporation for Assigned Names and Numbers – podmiot odpowiedzialny za przyznawanie nazw domen internetowych, ustalania ich struktury oraz sprawujący ogólny nadzór nad działaniem

[371] DOLiS-035-1535/13

serwerów Domain Name Servers na całym świecie). ICANN zarządza domenami najwyższego poziomu (ang. Top Level Domain), w tym również domeną „com". Podmioty takie dokonują w imieniu abonenta rejestracji nazw domenowych w domenach TLD zarządzanych przez ICANN (t.j. „com", „org", „info", „biz" oraz „net"), na podstawie umowy o rejestrację domeny, zawieranej pomiędzy rejestratorem a abonentem nazwy domenowej.

Natomiast w umowach zawieranych pomiędzy rejestratorami nazw domen internetowych a ICANN (tzw. umowy akredytacyjne) przewidziany jest obowiązek pozyskania przez rejestratora informacji na temat abonenta domeny w zakresie określonym przez ICANN (aktualnie zakres informacji o abonencie nazwy domenowej obejmuje jego imię i nazwisko, adres pocztowy, adres poczty elektronicznej, numer telefonu i ewentualnie numer faksu), a następnie przekazania ich do publicznie dostępnej bazy WHOIS oraz odpowiedniego ich poprawiania lub uaktualniania przez okres, w którym określona nazwa domenowa objęta jest rejestracją (pkt 3.3.7 ww. porozumienia akredytacyjnego). Niezależnie od obowiązku przekazywania przez rejestratorów nazw domen internetowych danych abonentów do bazy danych WHOIS, podmioty takie oferują często usługę polegającą na ograniczeniu zakresu lub ukryciu danych abonenta, dostępnych w wynikach bazy WHOIS (tzw. usługa „ID PROTECT). W przypadku skorzystania z takiej usługi w bazie WHOIS wyświetlane są wyłącznie dane rejestratora określonej nazwy domenowej oraz wskazanie, że jej abonentem jest osoba fizyczna (status nazwy domenowej: „INDIVIDUAL").

Odpowiadając na pytania GIODO miał okazję odnieść się również do kwestii **przetwarzania danych w chmurze** (*cloud computing*). Wskazał, że ta forma przetwarzania danych osobowych z pewnością w najbliższych latach będzie coraz bardziej popularna, m.in. ze względu na duże korzyści organizacyjne i ekonomiczne związane z jej stosowaniem. Korzyści ekonomiczne nie mogą prowadzić do tego, żeby dane osobowe przestały być właściwie przetwarzane, w tym stosowanie chronione, dlatego też obowiązek stosowania w tym zakresie zasad wynikających z powszechnie obowiązujących przepisów prawa pozostaje aktualny, niezależnie od sposobu, czy też formy ich przetwarzania. Samo przetwarzanie w chmurach jest prawnie dopuszczalne również z punktu widzenia przepisów ochrony danych osobowych, jakkolwiek administrator danych osobowych (czyli użytkownik

chmury) powinien mieć zapewnione uprawnienia kontrolne względem dostarczyciela chmury, co w praktyce może nastręczać wiele trudności[372].

Przechowywanie i przetwarzanie danych osobowych w chmurze obliczeniowej niesie ze sobą nowe ryzyka. Istnieje też stosunkowo pilna potrzeba objęcia tej materii stosownymi regulacjami prawnymi. Natomiast w chwili obecnej, zgodnie z obowiązującymi przepisami, na mocy ogólnego przepisu art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, administrator może powierzyć innemu podmiotowi, w drodze mowy zawartej na piśmie, przetwarzanie danych. Generalny Inspektor Ochrony Danych Osobowych stoi na stanowisku, że jest to także możliwe w przypadku przetwarzania danych w chmurze. Niemniej jednak w podanych przypadkach odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych, co jednak nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. Należy mieć także zawsze na uwadze obowiązek wynikający z art. 38 ustawy, który głosi, że administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Na zakończenie warto nadmienić, że w analizowanym okresie sprawozdawczym, podobnie jak w latach ubiegłych, nadal liczne były pytania dotyczące **rejestracji zbiorów danych osobowych (**w przedmiocie wątpliwości odnośnie istnienia, bądź nieistnienia obowiązku rejestracyjnego) oraz **marketingu** – w przedmiocie jego szeroko rozumianej legalności, w tym możliwości zgłoszenia sprzeciwu wobec przetwarzania danych osobowych w celach marketingowych lub możliwości odwołania zgody. W dalszym ciągu przedmiotem licznych kontrowersji z punktu widzenia ochrony danych osobowych była **działalność windykacyjna** w przedmiocie środków stosowanych przez firmy w celu odzyskania należności od dłużnika, ze szczególnym uwzględnieniem publikowania niektórych danych osobowych dłużnika w celu dokonania cesji wierzytelności.

[372] W tym miejscu należy wskazać, że wiele interesujących informacji odnoszących się do kwestii przetwarzania danych w chmurze dostępnych jest na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych www.giodo.gov.pl/plik/id_p/2689/j/pl/ oraz www.giodo.gov.pl/plik/id_p/2267/j/pl/, gdzie znajduje się tekst Memorandum (dokumentu roboczego w sprawie przetwarzania danych w chmurze obliczeniowej – kwestii ochrony danych i prywatności) Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji oraz treść wywiadu z Generalnym Inspektorem Ochrony Danych Osobowych. Pod adresem www.giodo.gov.pl/plik/id_p/2820/j/pl/ znaleźć można Opinię 5/2012 Grupy Roboczej Artykułu 29 ds. Ochrony Danych w sprawie przetwarzania danych w chmurze obliczeniowej.

8.1.8. 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 2013 roku Generalny Inspektor Ochrony Danych Osobowych skierował **121 takich wystąpień.**

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

Wśród nich znalazło się w**ystąpienie z dnia 8 marca 2013 r. do Ministra Sprawiedliwości w sprawie konieczności respektowania prawa do prywatności oraz ochrony informacji dotyczących osób obsługiwanych w punktach obsługi interesantów w sądach powszechnych**[373]**.** Powodem tego wystąpienia były zgłaszane Generalnemu Inspektorowi zastrzeżenia i wątpliwości dotyczące tworzenia lub zamiaru utworzenia w niektórych sądach biur obsługi interesantów w jednym pomieszczeniu z czytelnią akt lub biurami podawczymi oraz obawami, co do możliwości zachowania poufności danych osobowych i poszanowania prywatności osób obsługiwanych w pomieszczeniach sądu, które pełnić miałyby jednocześnie kilka ww. funkcji. Obawy te związane były przede wszystkim z koniecznością przekazywania w obecności innych osób szczegółowych informacji przez

[373] DOLiS-035-110/13

interesantów i interesantom na temat wszczynanych czy prowadzonych postępowań sądowych.

Możliwość tworzenia punktów obsługi interesantów, jeżeli pozwalają na to warunki kadrowe i lokalowe sądu, przewiduje § 544a ust. 1 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. 2003.5.22 z późn. zm.). Stosownie do ust. 2 cytowanego paragrafu w sądach, w których sporządza się protokół za pomocą urządzeń rejestrujących dźwięk oraz obraz i dźwięk, prezesi sądów utworzą punkty obsługi interesantów wraz ze stanowiącą ich integralną część czytelnią akt. W przypadku, gdy sprzeciwiają się temu warunki lokalowe i kadrowe należy utworzyć stosowne stanowisko w sekretariacie zapewniającym obsługę biurową danego wydziału. W ustępie 3 tego paragrafu określone zostały zadania punktów obsługi interesantów: m.in. informowanie o sposobach wszczęcia postępowania i podstawowych dokumentach, które należy złożyć przy wnoszeniu sprawy do sądu, kosztach sądowych, sposobie ubiegania się o zwolnienie od kosztów sądowych, przesłankach ustanowienia obrońcy, adwokata lub radcy prawnego z urzędu, rodzajach środków odwoławczych i terminach do ich wniesienia, o terminach i miejscach rozpraw (pkt 1).

Generalny Inspektor wskazał, że z przepisów prawa, w tym unormowań ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) wynika obowiązek poszanowania prywatności oraz tajemnicy danych osobowych. Zgodnie z art. 36 ust. 1 ustawy o ochronie danych osobowych, administrator danych musi podjąć takie środki organizacyjne i techniczne, aby zapewnić przetwarzanym danym osobowym właściwą ochronę przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Określone przez administratora danych zasady, środki i rozwiązania organizacyjne mające zapewnić danym bezpieczeństwo muszą być przestrzegane przez wszystkie osoby, które zgodnie z art. 37 ustawy o ochronie danych osobowych zostały upoważnione przez administratora danych do przetwarzania danych. Tylko bowiem takie osoby mogą mieć dostęp do danych osobowych. Osoby te powinny być wymienione w ewidencji osób upoważnionych do ich przetwarzania określonej w art. 39 ust. 1 ustawy i są one obowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia (art. 39 ust. 2).

Realizacja obowiązku właściwego zabezpieczenia danych osobowych oznacza między innymi przyjęcie takiego sposobu ich przetwarzania, który wyeliminuje możliwość zapoznania się z danymi przez osoby do tego nieupoważnione. Podkreślenia wymaga, że dobór odpowiednich środków organizacyjnych i technicznych w omawianym zakresie powinien uwzględniać charakter przetwarzanych danych, co oznacza, że w przypadku danych tzw. „sensytywnych", wymienionych w art. 27 ust. 1 ustawy, zastosowane środki powinny zapewniać im bardziej intensywną ochronę. W omawianej sytuacji, podczas rozmów z interesantami, w tym stronami postępowań sądowych, niewątpliwie może dochodzić do przekazywania danych sensytywnych[374].

W przedmiotowym wystąpieniu Generalny Inspektor Ochrony Danych Osobowych wskazał również na art. 26 ust. 1 pkt 1 i 2 ustawy o ochronie danych osobowych, zgodnie z którym administrator danych zobowiązany jest do dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Wskazuje ponadto, że obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, oraz zapewnienia danym bezpieczeństwa, musi być przestrzegany przez cały czas, w jakim trwa proces przetwarzania danych. Innymi słowy - obowiązki te nie ograniczają się jedynie do wprowadzenia przez administratorów odpowiednich zasad i sposobów postępowania z danymi osobowymi, ale również do stałego dbania i monitorowania, czy ustalone zasady i sposób organizacji są przestrzegane, a zatem czy proces przetwarzania danych przebiega prawidłowo.

Określone w ustawie obowiązki administratora danych zakreślone zostały w sposób ogólny i dyspozytywny. Stąd rozwiązanie problemu zachowania „prywatności" czy tajemnicy informacji przekazywanych interesantom i przez interesantów w zasadzie leży w gestii konkretnego administratora danych i może nastąpić na różne sposoby. Przykładowym rozwiązaniem w tym zakresie jest zapewnienie tej obsługi w oddzielnym pomieszczeniu lub

[374] Stosownie do art. 27 ust. 1 ustawy o ochronie danych osobowych, danymi sensytywnymi są dane ujawniające 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. Z tego względu tym bardziej nie podlega dyskusji konieczność respektowania prawa do prywatności oraz ochrony informacji obsługiwanych interesantów, w tym również takie organizowanie tej obsługi, aby prawa te były uszanowane.

przy wyizolowanych stanowiskach, przy których obsługiwany znajduje się w takiej odległości od reszty osób przebywających w pomieszczeniu, że nie jest możliwe zapoznanie się przez te osoby z treścią przekazywanych informacji.

Mając powyższe na uwadze Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Ministra Sprawiedliwości z prośbą o zasygnalizowanie potrzeby uwzględnienia powyższych uwag i powołanych przepisów podczas tworzenia i późniejszego funkcjonowania punktów obsługi interesanta w sądach powszechnych. W trosce o poszanowanie praw do prywatności osób obsługiwanych i ochronę informacji ich dotyczących, w biurach obsługi interesanta powinny znaleźć zastosowane jedynie takie rozwiązania, które pozostają w zgodzie z powyżej powołanymi przepisami.

W odpowiedzi Minister Sprawiedliwości poinformował, że odpis wystąpienia został przesłany prezesom Sądów Apelacyjnych celem zapoznania z nim prezesów i dyrektorów sądów powszechnych. Minister Sprawiedliwości zadeklarował również skierowanie wystąpienia do Dyrektora Krajowej Szkoły Sadownictwa Prokuratury o uwzględnienie w planie szkoleń dla urzędników sądowych problematyki poszanowania prawa interesantów do prywatności.

Celem wystąpienia skierowanego do **Ministra Spraw Wewnętrznych w dniu 15 marca 2013 r.**[375]**,** było zwrócenie uwagi na potrzebę podjęcia **prac legislacyjnych zmierzających do zmiany przepisów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 22 czerwca 2011 r. w sprawie usuwania pojazdów pozostawionych bez tablic rejestracyjnych lub których stan wskazuje na to, że nie są używane (Dz. U. z 2011 r. Nr 143, poz. 845 z późn. zm.) w zakresie udostępnienia danych osobowych właścicieli pojazdów, w celu usprawnienia działań podmiotów publicznych uczestniczących w działaniach określonych jego przepisami.**

Zgodnie z przepisami rozporządzenia, jednym z elementów procedury związanej z usunięciem pojazdu z drogi przez straż miejską (gminną), bądź Policję, jest niezwłoczne powiadomienie o tym fakcie właściwy miejscowo organ gminy, wraz z przesłaniem mu kopii dyspozycji usunięcia pojazdu, stanowiącej załącznik do rozporządzenia. Zgodnie z § 4 ust. 2 rozporządzenia, organ gminy, po otrzymaniu kopii dyspozycji, niezwłocznie podejmuje czynności mające na celu ustalenie właściciela pojazdu. Organ ten pisemnie powiadamia

[375] DOLiS-035-553/13

właściciela pojazdu o usunięciu pojazdu oraz o skutkach nieodebrania pojazdu w terminie określonym w art. 50a ust. 2 ustawy i każdorazowej konieczności uiszczenia należności za jego usunięcie. Przepis ten wyraźnie wskazuje, który organ ma nie tylko prawo, ale też obowiązek podejmowania czynności zmierzających do ustalenia właściciela pojazdu. Jednocześnie brak jest w tym akcie prawnym wskazania źródeł koniecznych informacji, w tym, brak jest wprost wskazania uprawnienia dla straży gminnych (miejskich), czy Policji do przekazywania/udostępniania danych osobowych zarówno co do zasady, jak i w przypadkach indywidualnych. Efektem powyższego, właściwe organy gminy zobligowane są do pozyskiwania informacji – danych osobowych właścicieli pojazdów w szczególności z centralnej ewidencji pojazdów, dla której administratorem danych pozostaje minister właściwy do spraw wewnętrznych. Tym samym, straże miejskie, czy Policja, jako podmioty uprawnione do usunięcia pojazdu i w toku czynności zmierzających do usunięcia pojazdu ustalające jego właściciela celem potwierdzenia zajścia okoliczności uzasadniających usunięcie pojazdu nie posiadają uprawnienia do przekazania tych informacji właściwym organom gminy.

W przedmiotowym wystąpieniu organ do spraw ochrony danych osobowych poddał rozwadze sposób rozwiązania istniejącego problemu w drodze odpowiedniej nowelizacji rozporządzenia w sprawie usuwania pojazdów pozostawionych bez tablic rejestracyjnych lub których stan wskazuje na to, że nie są używane, zmierzającej do przyznania podmiotom współpracującym w tym zakresie, kompetencji udostępniania informacji stanowiących dane osobowe właścicieli usuwanych pojazdów. W ocenie GIODO, istniejące normy kompetencyjne wydają się nie uwzględniać w pełni interesu państwa. Ich konstrukcja wydaje się wydłużać całą procedurę, zwiększając obciążenia podmiotów ją stosujących. Należy także podkreślić, iż podmioty publiczne winny działać na podstawie przepisów prawa, w ramach kompetencji nadanych im tymi przepisami (art. 7 Konstytucji RP, art. 6 ustawy Kodeks postępowania administracyjnego). W przypadku podmiotów publicznych zarówno zakres, jak i cel przetwarzania danych osobowych jest najczęściej wyznaczony przepisami prawa i wynika on bezpośrednio z określonych prawem zadań danego podmiotu. Zasada ta nakazuje, by wszelkie działania organów władzy publicznej były oparte na wyraźnie określonych normach kompetencyjnych. Obowiązujące natomiast postanowienia w tym zakresie budzą wątpliwości co do wypełnienia przez nie ww. wymogów przejrzystości norm prawa.

W odpowiedzi Minister Spraw Wewnętrznych pismem z dnia 15 kwietnia 2013 r. (DN-NKSPP-0748-11/2013/PD) poinformował GIODO o tym, iż „przeprowadzona zostanie analiza mająca na celu wypracowanie możliwych kierunków zmian w prawie, w wyniku których nastąpiłoby uregulowanie sprawy przekazywania przez organy usuwające pojazd, danych osobowych jego właściciela, organom właściwej gminy".

Na uwagę zasługuje wystąpienie GIODO z dnia 24 maja 2013 r. do jednej ze spółdzielni mieszkaniowych[376] w związku ze skargą na udostępnienie danych osobowych skarżącej osobom do tego nieupoważnionym, poprzez wywieszenie pism zawierających jej dane osobowe w holu nieruchomości należącej do spółdzielni.

W ocenie Generalnego Inspektora doszło w ten sposób do naruszenia przepisów ustawy o ochronie danych osobowych. Spółdzielnia bowiem, jako administrator danych osobowych, była zobowiązana respektować zasady przetwarzania danych osobowych i ponosiła odpowiedzialność za podejmowane działania. Poprzez wywieszenie na tablicy ogłoszeń w holu ww. nieruchomości pism skarżącej zawierających jej dane osobowe, spółdzielnia dopuściła do sytuacji, w której osoby nieupoważnione - mające dostęp do tego miejsca - mogły zapoznać się z upublicznionymi w ten sposób informacjami. Takie udostępnianie danych jest niezgodne zarówno z przepisami ustawy o ochronie danych osobowych, jak również z przepisami ustawy z dnia 16 września 1982 r. prawo spółdzielcze (Dz. U. z 2003 r. Nr 188, poz. 1848 z późn. zm.), czy też ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2003 r. Nr 1116, poz. 119). Przepisy ww. ustaw wskazują warunki, w jakich osoby upoważnione mogą zapoznać się z danymi spółdzielców. Nie są to dane powszechnie dostępne.

Wobec powyższego organ do spraw ochrony danych osobowych stwierdził, że działania spółdzielni, polegające na dopuszczeniu do zawieszenia w holu nieruchomości zarządzanej przez spółdzielnię pism zawierających dane osobowe skarżącej, naruszyły zasady dotyczące przetwarzania danych osobowych, wyznaczone przepisami art. 23 ust. 1 oraz art. 36 ustawy o ochronie danych osobowych. Spółdzielnia ma obowiązek czuwać nad tym, aby działania poszczególnych jej organów nie naruszały przepisów prawa powszechnie obowiązującego, w tym zasad wynikających z ustawy o ochronie danych osobowych. Niezastosowanie się do zasad wynikających z ustawy może skutkować zarówno odpowiedzialnością karną, jak i cywilną przez osoby odpowiedzialne za przetwarzanie danych osobowych. Zgodnie z brzmieniem art. 51

[376] Pismo GIODO z dnia 24 maja 2013 r. (znak: DOLiS-440-982/12/OS/I/32766)

ustawy o ochronie danych osobowych, kto administrując zbiorem danych lub będąc zobowiązanym do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (ust.1). Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (ust. 2).

W odpowiedzi na powyższe spółdzielnia wskazała, iż zastosowała się do wskazanych przez GIODO wytycznych i podkreśliła, iż w podejmowanych przez siebie czynnościach będzie przestrzegać przepisów ustawy o ochronie danych osobowych w celu uniknięcia podobnych sytuacji na przyszłość.

Z kolei w**ystąpienie z dnia 27 maja 2013 r.**[377] **skierowane do Ministra Administracji i Cyfryzacji dotyczyło wzorów deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi kształtujących zakres danych osobowych pozyskiwanych od mieszkańców gminy.**

Wystąpienie zostało skierowane do Ministra Administracji i Cyfryzacji, jako organu odpowiedzialnego za nadzór nad działalnością wojewodów na podstawie kryterium zgodności ich działania z powszechnie obowiązującym prawem (art. 8 ust. 3 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie – Dz. U. Nr 31, poz. 206 z późn. zm.). Przedmiotem wystąpienia było zasygnalizowanie Ministrowi Administracji i Cyfryzacji potrzeby wskazania wojewodom pełniącym funkcję organu nadzoru nad działalnością jednostek samorządu terytorialnego pod względem legalności (art. 3 pkt 3 i 4 ww. ustawy) na konieczność respektowania przepisów o ochronie danych osobowych w treści uchwał organów jednostek samorządu terytorialnego, określających m.in. wzory deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi kształtujących zakres danych osobowych pozyskiwanych od mieszkańców gminy.

Mocą znowelizowanych – poprzez ustawę z dnia 1 lipca 2011 r. o zmianie ustawy o utrzymaniu czystości i porządku w gminach oraz niektórych innych ustaw (Dz. U. Nr 152, poz. 897) – przepisów ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2012 r. poz. 391 z późn. zm.), gminy zobowiązane zostały do zorganizowania odbierania odpadów komunalnych od właścicieli nieruchomości, na których zamieszkują mieszkańcy (art. 6c ust. 1). Następnie, art. 6m ust. 1 tego aktu prawnego obliguje

[377] DOLiS-072-12/13

właścicieli nieruchomości do złożenia do wójta, burmistrza lub prezydenta miasta deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w terminie 14 dni od dnia zamieszkania na danej nieruchomości pierwszego mieszkańca lub powstania na danej nieruchomości odpadów komunalnych. Przy czym każda zmiana informacji będących podstawą ustalania wysokości należnej opłaty stanowi podstawę do wypełnienia i dostarczenia właściwym organom nowej deklaracji (ust. 2).

Ustawodawca przewidział także w art. 6n ust. 1 znowelizowanej ustawy, iż rada gminy, uwzględniając konieczność zapewnienia prawidłowego obliczenia wysokości opłaty za gospodarowanie odpadami komunalnymi oraz ułatwienia składania deklaracji, określać ma w drodze uchwały stanowiącej akt prawa miejscowego m.in. wzór deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanej przez właścicieli nieruchomości. Dalsze przepisy przyznają także radzie gminy uprawnienie do określania w drodze ww. uchwały wykazu dokumentów potwierdzających dane zawarte w deklaracji (ust. 2 tego przepisu).

Rada gminy (po zasięgnięciu opinii państwowego powiatowego inspektora sanitarnego) została zobowiązana, stosownie do treści art. 4 ust. 1 ustawy, do uchwalenia regulaminu utrzymania czystości i porządku na terenie gminy, jako aktu prawa miejscowego. Regulamin ten określa szczegółowe zasady utrzymania czystości i porządku na terenie gminy dotyczące m.in. rodzaju i minimalnej pojemności pojemników przeznaczonych do zbierania odpadów komunalnych na terenie nieruchomości oraz na drogach publicznych, warunków rozmieszczania tych pojemników i ich utrzymania w odpowiednim stanie sanitarnym, porządkowym i technicznym, przy uwzględnieniu m.in. liczby osób korzystających z tych pojemników (art. 4 ust. 2 pkt 2b). Dalsze przepisy tej ustawy precyzują, iż opłata za gospodarowanie odpadami komunalnymi stanowi iloczyn: 1) liczby mieszkańców zamieszkujących daną nieruchomość, lub 2) ilości zużytej wody z danej nieruchomości, lub też 3) powierzchni lokalu mieszkalnego oraz stawki opłaty ustalonej na podstawie art. 6k ust. 1.

Z powyższego wynika, iż rada gminy może w drodze uchwały (jako aktu prawa miejscowego w rozumieniu art. 87 ust. 1 ustawy z dnia 2 kwietnia 1997 r. – Konstytucja Rzeczypospolitej Polskiej) nakładać na mieszkańców – właścicieli nieruchomości – pewne obowiązki w zakresie konieczności przedkładania informacji służących do ustalenia wysokości opłat za gospodarowanie przez nich odpadami komunalnymi.

Mając na uwadze powyższe przepisy Generalny Inspektor zauważył, iż uchwała może jedynie konkretyzować ducha ustawy, określającego zasady i wyznaczającego zakres obowiązków organów gminy z jednej strony oraz mieszkańców gminy – właścicieli nieruchomości z drugiej. Nie może jednak kształtować przedmiotowych obowiązków w sposób dowolny, wbrew pierwotnym uprawnieniom ustawowym, z pominięciem tzw. 1) zasady legalizmu, 2) zasady adekwatności oraz 3) zasady celowości stanowiących jeden z filarów demokratycznego państwa prawnego, którym jest Rzeczpospolita Polska i mających swe źródło w polskiej ustawie zasadniczej, tj. Konstytucji Rzeczypospolitej Polskiej.

Generalny Inspektor wskazał, że poszanowanie przez organy gminy zasady legalizmu powinno mieć odzwierciedlenie m.in. w uwzględnianiu w wydawanych przez nie uchwałach obowiązujących przepisów prawa, tak międzynarodowych, konstytucyjnych, jak i ustawodawstwa zwykłego – w tym przypadku w szczególności ustawy o utrzymaniu czystości i porządku w gminach. Skoro zaś ostatni ze wspomnianych aktów prawnych, w związku z wykonywaniem przez te organy swych obowiązków w zakresie gospodarowania odpadami, posługuje się pojęciem danych właścicieli nieruchomości oraz „liczbą mieszkańców danej gminy", to niedopuszczalne pozostaje nakładanie przez gminy na tychże właścicieli obowiązku przedkładania deklaracji zawierających dane osobowe osób zamieszkujących wspólnie z nimi. Brak jest bowiem podstawy prawnej do przetwarzania o wspomnianych osobach trzecich innych, niż liczbowe, informacji, w tym konkretnych danych osobowych.

Tymczasem z docierających do Generalnego Inspektora Ochrony Danych Osobowych sygnałów wynikało, iż niektóre gminy, określając wzór deklaracji o wysokości opłat za gospodarowanie odpadami komunalnymi, wymagają podania w ich treści danych osobowych osób zamieszkujących wspólnie z właścicielem w zakresie imion, nazwisk, numerów PESEL, a także wskazują na konieczność zamieszczania w nich danych na temat nazwy pracodawcy lub innych źródeł dochodów tych osób, co budzi największe zdziwienie Generalnego Inspektora Ochrony Danych Osobowych oraz wątpliwości pod kątem legalności takich działań. Co więcej, w wielu przypadkach zakres pozyskiwanych informacji jest rozszerzany poprzez żądanie przedłożenia kopii określonych dokumentów, stanowiących załączniki do deklaracji. Przedmiotem żądania stają się więc zaświadczenia z uczelni wyższych mających siedzibę poza granicami danej miejscowości, potwierdzające odbywanie także przez te osoby nauki w określonym systemie (studia stacjonarne/niestacjonarne), zaświadczenia od

pracodawcy potwierdzające stałe wykonywanie pracy poza daną miejscowością w sytuacji, gdy jej wykonywanie związane jest z zamieszkaniem poza terenem gminy, czy zaświadczenia z właściwej wojskowej jednostki organizacyjnej o odbywaniu służby wojskowej lub inne dokumenty potwierdzające stałą nieobecność mieszkańca na terenie posesji lub lokalu wystawione przez „odpowiednie instytucje". Wśród powyższych może więc się znaleźć zaświadczenie np. z domu dziecka, zakładu karnego czy placówki opieki zdrowotnej.

Ponadto wśród deklaracji, za pomocą których zbierane są dane osobowe, znajdują się także te zawierające oświadczenia o świadomości odpowiedzialności karnej określonej w art. 233 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 88, Nr 553 z późn. zm.) za podanie nieprawdziwych informacji, wymagające podpisania przez składającego, a inne dodatkowo klauzulę zgody na przetwarzanie danych osobowych „zgodnie z art. 23 ust. 1 ustawy (…) o ochronie danych osobowych (…)".

Mając powyższe na uwadze Generalny Inspektor Ochrony danych osobowych z całą stanowczością stwierdził, iż nie jest dopuszczalne zawieranie rygoru odpowiedzialności karnej w treści deklaracji, który to rygor mógłby wynikać co najwyżej z treści aktu rangi ustawy, nie zaś autorytarnego uznania organów gminy – choćby poprzez jego ujęcie we właściwych przepisach uchwały – oraz zamieszczanie klauzuli zgody na przetwarzanie danych osobowych w treści deklaracji.

Generalny Inspektor Ochrony Danych Osobowych wskazał również, że z kolei zgoda osoby, której dane dotyczą w takiej, jak opisywana sytuacji, nie może być podstawą przetwarzania danych osobowych z dwóch powodów. Po pierwsze, skoro organy władzy publicznej działają na podstawie i w granicach prawa (art. 7 Konstytucji RP), to również organy gminy opierać muszą swoje działanie na przesłance legalności wskazanej – w zależności od kategorii przetwarzanych danych – w art. 23 ust. 1 pkt 2 (w stosunku do tzw. danych zwykłych, jak np. imię, nazwisko, adres zamieszkania, numer PESEL) lub w art. 27 ust. 2 pkt 2 ustawy (jeżeli chodzi o dane nazywane szczególnie chronionymi, wymienione w art. 27 ust. 1 ustawy, do których zalicza się m.in. dane dotyczące stanu zdrowia, czy orzeczeń wydanych w postępowaniu sądowym lub administracyjnym). Przepisy te wymagają istnienia odpowiedniej podstawy mającej swe źródło w przepisach prawa, w tym – w przepisach rangi ustawy, jeżeli przedmiotem przetwarzania stają się dane szczególnie chronione, wymienione we wskazanym art. 27 ust. 1 ustawy. Powyższe zyskuje na znaczeniu właśnie w kontekście pozyskiwania przez gminy, na podstawie przepisów wydawanych

uchwał, danych osobowych, które stanowią dane szczególnie chronione (np. zaświadczenie z zakładu karnego czy aresztu śledczego potwierdzającego przebywanie określonej osoby poza miejscem zamieszkania). Zgoda osoby, której dane dotyczą mogłaby stanowić podstawę przetwarzania danych osobowych w takiej sytuacji, kiedy o „marginesie" pozyskiwania i dalszego przetwarzania danych osobowych nie zadecydowano w treści określonego aktu prawnego. Za pomocą zgody osoby, której dane dotyczą, nie można bowiem „uzupełniać" prawodawcy. Po wtóre zaś, w sytuacji, gdy zgoda osoby na przetwarzanie danych osobowych nie stanowi prawidłowo złożonego oświadczenia woli trudno mówić o wypełnieniu wszystkich elementów zgody, o których traktuje art. 7 pkt 5 ustawy o ochronie danych osobowych, i możliwości wskazywania na tę przesłankę jako podstawę przetwarzania danych osobowych.

W ocenie GIODO trudno było założyć, iż zamieszczona w treści określonego formularza (np. deklaracji) klauzula w przedmiocie zgody na przetwarzanie danych osobowych, czyni zadość powyższym kryteriom. Osoba, której dane dotyczą, podpisująca formularz, nie ma bowiem możliwości tak odmówić wyrażenia zgody na przetwarzanie jej danych osobowych, jak i ewentualnego odwołania uprzednio wyrażonej zgody. Zamieszczenie w treści formularza przedmiotowej klauzuli wprowadza więc osoby, których dane dotyczą, w błąd co do – po pierwsze – możliwości, a po wtóre – konsekwencji niewyrażenia zgody.

Powyższe wątpliwości pozostają zasadne tym bardziej, iż wobec wypełniania tak skonstruowanej deklaracji, za pośrednictwem której pozyskiwane są również dane osobowe osób trzecich, obejmującej oświadczenie woli w przedmiocie zgody na przetwarzanie danych osobowych, dochodzi do sytuacji, w której właściciel nieruchomości, wyrażając taką zgodę poprzez podpisanie zamieszczonego oświadczenia, czyni to nie tylko w swoim imieniu, ale także w imieniu tychże osób trzecich, wspólnie z nim zamieszkujących. Nie sposób pominąć również faktu, że ustawodawca posługując się pojęciem „deklaracja" wyraźnie wskazał, że podstawą działania jest oświadczenie składane przez osobę fizyczną, nie zaś zbiór zaświadczeń przedkładanych dla opisania stanu faktycznego. Każda sytuacja, w której zamiast deklaracji (lub obok niej) przedstawiać należy inne dokumenty musi wynikać ze szczególnych przesłanek, opisanych na poziomie ustawy. W kontekście zasady adekwatności organ ochrony danych osobowych wskazał, że jakkolwiek bowiem uchwała może uprawniać organy gminy do żądania od właścicieli nieruchomości danych natury

zwykłej (imię, nazwisko, adres zamieszkania) to nie może jednocześnie zezwalać na pozyskiwanie danych w nadmiarze, danych nieadekwatnych w stosunku do celu ich przetwarzania, a co za tym idzie – oczywiście zbędnych. Organy gminy, jako administratorzy danych w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, dla uznania legalności ich działania muszą bowiem, poza wykazaniem istnienia podstawy prawnej upoważniającej do przetwarzania przez nich danych osobowych, uczynić zadość tzw. zasadzie adekwatności danych w stosunku do celów ich przetwarzania, określonych w art. 26 ust. 1 pkt 3 tej ustawy. Adekwatność danych w stosunku do celu ich przetwarzania powinna być natomiast rozumiana jako równowaga pomiędzy dobrem osoby, której dane dotyczą, a interesem administratora danych. W licznych przypadkach uchwalane przez właściwe organy jednostek samorządu terytorialnego akty prawa miejscowego odnoszące się do opisywanej materii, naruszają natomiast wspomnianą zasadę poprzez np. obligowanie właścicieli nieruchomości do podawania nadmiernie szerokiego zakresu danych. Niektóre gminy żądają informacji począwszy od tych dotyczących dat urodzenia, nazwisk rodowych, imion ojca oraz matki właściciela nieruchomości, numeru księgi wieczystej i numeru geodezyjnego działki, a skończywszy na danych dotyczących kont bankowych (np. pełny numer rachunku bankowego właściciela nieruchomości).

W poszczególnych deklaracjach pojawiają się również pola, których wypełnienie pozostaje obowiązkiem, zamiast wyłącznie możliwością. Tak jest w sytuacji żądania przedkładania informacji o numerze telefonu czy adresie poczty elektronicznej danego właściciela. Powyższe pozostaje wątpliwe, albowiem nie jest dopuszczalne pośrednie zobowiązywanie tej grupy osób do posiadania telefonu czy poczty elektronicznej. Nie kwestionując fakultatywności podawania tego typu informacji w treści deklaracji, nie można jednocześnie wyrazić aprobaty wobec ich wymuszania poprzez wprowadzenie obowiązkowego pola w deklaracji, przesądzającego o konieczności zamieszczania tego typu informacji o właścicielach nieruchomości. Tego typu dane powinny być traktowane jako fakultatywne.

W kontekście zasady legalizmu oraz adekwatności danych w stosunku do celów ich przetwarzania, Generalny Inspektor zwrócił również uwagę na problem weryfikowania spełniania przez właścicieli nieruchomości obowiązku segregowania odpadów poprzez zamieszczanie na workach do zbierania tychże odpadów lub stosownych kontenerach kodów kreskowych czy chipów. Podkreślił, że używanie różnego rodzaju procedur

zautomatyzowanych opartych na danych przywiązywanych do pojemników pozostaje poza materią ochrony danych osobowych jedynie wówczas, kiedy opatrzony etykietą produkt pozostaje w łańcuchu logistycznym i nie może być powiązany z osobą. Tylko wówczas specyficzny dla produktu numer na etykiecie nie stanowi danych osobowych. Kiedy natomiast te dane zostaną przetworzone w określonym podmiocie razem z danymi identyfikującymi konkretną osobę, takie dane zostaną zazwyczaj sklasyfikowane jako dane osobowe. Jest to szczególnie istotne w razie wykorzystywania do celu segregacji śmieci technik RFID (Radiowa Identyfikacja Obiektów - Radio Frequency Identification). Używanie chipów RFID i ich czytników jest z pewnością innowacyjnym i skutecznym rozwiązaniem, Należy jednak pamiętać, że w tej sytuacji bardzo prawdopodobne jest, że oznaczone chipem przedmioty (np. pojemniki) będą opatrywane danymi, które w powiązaniu z innymi danymi będącymi w gestii administratora mogą być danymi osobowymi. W takiej sytuacji po stronie administratora danych powstaje obowiązek stosowania w jego działalności wszystkich przepisów o ochronie danych osobowych. W szczególności, przed wprowadzeniem rozwiązań mających na celu stosowanie Radiowej Identyfikacji Obiektów jako mechanizmu przetwarzania danych osobowych należy – na każdym etapie tego procesu – rozważać wpływ konstruowanych rozwiązań na sferę prywatności (tzw. koncepcja privacy by design)[378], w tym również pod kątem stosowania prawidłowych zasad bezpieczeństwa przetwarzania danych osobowych.

Mając natomiast na uwadze zasadę celowości, wynikającą tak z przepisów międzynarodowych (art. 6 ust. 1b dyrektywy) jak i krajowych (art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych), stosownie do treści których administrator danych przetwarzający dane musi dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności zapewnić, aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, GIODO podkreślił, iż będące w posiadaniu organów gminy bazy danych właścicieli nieruchomości, zawierające ich dane osobowe gromadzone poprzez stosowne deklaracje, nie mogą przez te organy być wykorzystywane w jakimkolwiek innym celu, aniżeli konieczność

[378] Koncepcja *privacy by design* zakłada, iż najważniejsze problemy związane z ochroną prywatności w kontekście funkcjonowania podobnych systemów należy przewidywać już na etapie poprzedzającym ich budowę – od samego początku aż po zakończenie, a więc – co istotne – jeszcze przed rozpoczęciem pozyskiwania i dalszego przetwarzania danych osobowych. Powyższe umożliwia podejmowanie odpowiednich działań ukierunkowanych na zapobieganie występowaniu przedmiotowych problemów, zamiast następczego reagowania na pojawiające się nieprawidłowości.

realizacji obowiązków wynikających z powoływanej ustawy o utrzymaniu czystości i porządku w gminach.

Bezsprzecznym obowiązkiem organów gmin, które w drodze uchwał stanowią prawo poprzez akt prawa miejscowego, jest respektowanie wszystkich opisanych powyżej zasad przetwarzania i ochrony danych osobowych mieszkańców. Obowiązkiem zaś wojewodów – orzekanie o nieważności uchwał w sytuacji niezgodności zawartych w nich treści z przepisami prawa (art. 90 ust. 1 w związku z art. 91 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.).

Generalny Inspektor Ochrony Danych Osobowych mając świadomość pojawiających się nieprawidłowości w zakresie zbierania danych osobowych na podstawie uchwały rady gminy sprzecznej z przepisami o ochronie danych osobowych, zapowiedział w przedmiotowym wystąpieniu, że będzie podejmował właściwe działania zmierzające do przywrócenia stanu zgodnego z prawem i zapewnienia właściwej ochrony osobom, których dane dotyczą, w zakresie ich zgodnego z prawem przetwarzania, jak również przeprowadzi stosowne czynności kontrolne i w razie konieczności rozpocznie postępowania administracyjne w celu wydania decyzji administracyjnych, które zawierać mogą nakazy usunięcia ze zbiorów danych przetwarzanych z naruszeniem przepisów o ochronie danych osobowych bądź zmianę sposobu ich przetwarzania – w tym zmiany polegające na zakazie stosowania systemów teleinformatycznych przetwarzających dane sprzecznie z prawem.

W odpowiedzi na to wystąpienie, MAiC pismem z dnia 28 maja 2013 r. zapewnił o przekazaniu wystąpienia GIODO do Regionalnych Izb Obrachunkowych i wojewodów oraz poinformował, że zwrócił się do tychże o dokonanie przeglądu uchwał pod katem ochrony danych osobowych.

Warto w tym miejscu nadmienić, że powyższe wystąpienie Generalnego Inspektora Ochrony Danych Osobowych było działaniem podjętym między innymi w odpowiedzi na wiele wątpliwości i zapytań kierowanych do organu ochrony danych osobowych zarówno przez podmioty publiczne, jak i prywatne, a także przedstawicieli mediów. Po rozesłaniu tego wystąpienia do ww. adresatów, do organu ochrony danych osobowych oraz Ministra Administracji i Cyfryzacji wpłynęło pismo jednego z burmistrzów negujące stanowisko GIODO co do kwestii podniesionych w wystąpieniu[379]. Do przedstawionych zarzutów

[379] DOLiS-072-12/13

GIODO odniósł się w piśmie skierowanym do MAiC, kierując kopię odpowiedzi również do burmistrza. Wskazał w nim, iż opisane przez burmistrza działanie polegające za uznaniu zasadności pozyskiwania od mieszkańców gmin - w celu prawidłowego obliczenia wysokości opłaty za gospodarowanie odpadami komunalnymi - informacji dotyczących imienia ojca i matki, numeru NIP, czy daty urodzenia lub innych, szeroko opisanych przez GIODO w treści przywołanej we wstępie korespondencji, informacji o osobach, na wypadek toczącego się postępowania egzekucyjnego, stanowi jaskrawy przykład naruszenia jednej z naczelnych zasad przetwarzania danych osobowych, a mianowicie zasady adekwatności danych w stosunku do celów ich pozyskania, o której stanowi tak art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, jak i art. 6 ust. 1 lit. c dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.WE.23.11.1995). Jej poszanowanie wymaga bowiem, aby administrator danych każdorazowo przetwarzał dane osobowe wyłącznie w zakresie niezbędnym z punktu widzenia określonego celu przetwarzania danych. Swym rodzajem i treścią dane osobowe nie powinny zatem wykraczać poza potrzeby wynikające z celu ich zbierania. W glosie do wyroku Naczelnego Sądu Administracyjnego z dnia 19 grudnia 2001 r. (II SA 2869/00) A. Drozd podniósł, iż zbieranie danych osobowych na zapas, co do zasady narusza zasadę adekwatności, ponieważ takie postępowanie nie mieści się w ramach celu przetwarzania.

Cel wprowadzenia deklaracji i pozyskiwania za jej pośrednictwem danych osobowych jest niewątpliwy i w sposób wyraźny wynika z cytowanego przez burmistrza art. 6n ust. 1 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2012 r. poz. 391 z późn. zm.). Jest nim „konieczność zapewnienia prawidłowego obliczenia wysokości opłaty za gospodarowanie odpadami komunalnymi (…)". Jednakże celu przetwarzania danych osobowych w tym przypadku nie stanowi z całą pewnością skuteczne prowadzenie egzekucji w następstwie prawidłowo wypełnionego tytułu wykonawczego. Warto zważyć, iż prawo do przetwarzania danych w związku z koniecznością wszczęcia egzekucji administracyjnej powstaje z chwilą istnienia określonej zaległości. Trudno bowiem z góry zakładać, iż każdy z mieszkańców – osób, których dane dotyczą – będzie uchylać się od obowiązku wypełniania swych zobowiązań finansowych względem danej jednostki samorządu terytorialnego i będzie dłużnikiem, w stosunku do którego zostanie wszczęte postępowanie egzekucyjne.

Powyższe rozważania prowadzą do wniosku, iż w opisywanym przez burmistrza przypadku dochodzi do zbierania danych osobowych jeszcze przed zaistnieniem okoliczności usprawiedliwiających takie pozyskanie. Inaczej mówiąc, w chwili pozyskiwania danych nie istnieje cel, dla którego one są gromadzone i dalej przetwarzane. Tego typu działanie zabronione jest – podobnie, jak opisane powyżej pozyskiwanie danych wbrew „zasadzie adekwatności danych w stosunku do celu ich pozyskania" – mocą tak dyrektywy 95/46/WE, jak i polskiej ustawy o ochronie danych osobowych. Dyrektywa posługuje się pojęciem konieczności przetwarzania danych dla „określonych, jednoznacznych i legalnych celów" (art. 6 ust. 1 lit. b), zaś ustawa wymaga, aby dane osobowe były „zbierane dla oznaczonych, zgodnych z prawem celów" (art. 26 ust. 1 pkt 2). Trudno natomiast mówić o uczynieniu zadość tym obowiązkom przez administratora danych, który pozyskuje dane osobowe pomimo, że w danej chwili nie ma ku temu powodów. Cel, dla którego są one pozyskiwane, nie istnieje.

Należy podkreślić, iż w demokratycznym państwie prawnym urzeczywistniającym zasady sprawiedliwości społecznej jakim jest Rzeczpospolita Polska (art. 2 Konstytucji RP), władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach, niż niezbędne w demokratycznym państwie prawnym. Dopiero przejście tzw. „konstytucyjnego testu proporcjonalności" nie naraża podmiotu/organu wprowadzającego rozwiązania dotykające praw i wolności obywatelskich, na zarzut zbyt głębokiej ingerencji.

W zakresie rozumienia treści art. 51 ust. 2 Konstytucji RP wypowiadał się już wielokrotnie Trybunał Konstytucyjny. I tak w wyroku z dnia 20 listopada 2002 r. (sygn. akt K 41/02) Trybunał wskazał, że istnienie w przedmiotowym przepisie odrębnej regulacji dotyczącej proporcjonalności wkraczania w prywatność jednostki należy tłumaczyć tym, iż naruszenie autonomii informacyjnej poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce, jest typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki. Na powyższe nie ma i nie może mieć wpływu okoliczność, iż organy pozyskujące dane osobowe „są obowiązane do zachowania w tajemnicy pozyskanych informacji". Powyższe nie legalizuje bynajmniej żądania danych w nadmiarze, danych zbędnych i takich, których przetwarzanie jest niedopuszczalne. Obowiązek zachowania danych w tajemnicy jest obowiązkiem wtórnym w stosunku do konieczności legitymowania się pierwotnym prawem przetwarzania określonego zakresu

informacji. Dlatego też należy wskazać, iż zgodnie z art. 49 ust. 1 ustawy o ochronie danych osobowych, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 49 ust. 1).

W odpowiedzi na powyższe Ministerstwo Administracji i Cyfryzacji pismem z dnia 28 maja 2013 r. zapewniło o przekazaniu wystąpienia GIODO do Regionalnych Izb Obrachunkowych i wojewodów oraz że zobowiązało ich do dokonania przeglądu uchwał pod katem ochrony danych osobowych.

O zapewnienie prawidłowości procesu przetwarzania danych przechowywanych przez placówki hotelarskie[380] zwrócił się GIODO do Dyrektora Generalnego Polskiej Izby Hotelarstwa w Warszawie wystąpieniu z dnia 26 czerwca 2013 r.

Wystąpienie zostało skierowane związku ze zmianą przepisów o ewidencji ludności i dowodach osobistych, tj. nowelizacją 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.), dokonaną ustawą z dnia 7 grudnia 2012 r. o zmianie ustawy o ewidencji ludności i dowodach osobistych oraz niektórych innych ustaw (Dz. U. Nr 1407). Na mocy art. 1 pkt 10 ww. ustawy nowelizującej został uchylony rozdział 5 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.) określający obowiązek meldunkowy wczasowiczów i turystów, a w szczególności przepisy art. 18-22 ww. ustawy. Jednocześnie z mocy art. 1 pkt 18 ww. ustawy zmieniającej uchylony został art. 44b ustawy o ewidencji ludności i dowodach osobistych, który precyzował formę i zakres danych osobowych gromadzonych w zbiorze osób przebywających w obiektach, o których mowa w nieobowiązującym już art. 18 ww. ustawy. Na gruncie art. 1 pkt 22 ww. ustawy zmieniającej utracił moc art. 51 ust. 1 ustawy o ewidencji ludności i dowodach osobistych, który zawierał delegację ustawową do wydania rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 24 grudnia 2002 r. w sprawie zgłaszania i przyjmowania danych niezbędnych do zameldowania i wymeldowania oraz prowadzenia ewidencji ludności i ewidencji wydanych i utraconych dowodów osobistych (Dz. U. Nr 236, poz. 1999), co skutkuje utratą mocy wspomnianego aktu wykonawczego. Powyższe zmiany ww. przepisów weszły w życie z dniem 31 grudnia 2012 r. (art. 8 ww. ustawy nowelizującej).

[380] DOLiS-035-1621/13

Zameldowanie na pobyt czasowy trwający do 3 miesięcy dokonane na podstawie wspomnianej ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych, wygasa z dniem 31 grudnia 2012 r. (art. 6 ww. ustawy zmieniającej). Wprowadzenie przez ustawodawcę ww. zmian miało na celu wdrożenie proobywatelskich udogodnień w procedurze meldunkowej (zob. treść uzasadnienia ww. ustawy zmieniającej).

W przepisach obowiązującej ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych w brzmieniu nadanym ustawą z dnia 7 grudnia 2012 r. o zmianie ustawy o ewidencji ludności i dowodach osobistych oraz niektórych innych ustaw (Dz. U. Nr 1407), ustawodawca nie określił szczegółowych unormowań w stosunku do osób przebywających w danej miejscowości w celach turystyczno-wypoczynkowych. W związku z tym zastosowanie znajdują przepisy ogólne ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych. Przepis art. 10 ww. ustawy, który stanowi o obowiązku meldunkowym osoby przebywającej w danej miejscowości dłużej niż 3 miesiące (należy tego dokonać najpóźniej w 30. dniu liczonym od dnia przybycia do tego miejsca) znajduje zastosowanie także do osób przebywających w danej miejscowości w celach turystyczno-wypoczynkowych bez względu na to, czy korzystają z usług hotelu lub innego zakładu. Obowiązek meldunkowy dotyczy bowiem wszystkich osób przebywających w danej miejscowości dłużej niż 3 miesiące. Realizacja obowiązku meldunkowego następuje przed organem gminy właściwym ze względu na nowe miejsce pobytu (art. 11 i 12 ww. ustawy).

Art. 74 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. Nr 217, poz. 1427, z późn. zm.) przewiduje zniesienie obowiązku meldunkowego od dnia 1 stycznia 2016 r.

Organ do spraw ochrony danych osobowych zwrócił uwagę, że ustawa o ochronie danych osobowych obliguje podmioty przetwarzające dane osobowe w procesie każdego przedsięwzięcia związanego z przetwarzaniem danych osobowych do przestrzegania zasad wyrażonych w przepisach prawa, w tym przepisach ustawy o ochronie danych osobowych, na każdym etapie przetwarzania tych danych, w tym na etapie ich pozyskiwania, utrwalania, przechowywania i udostępniania.

Istotne z punktu widzenia zasad określonych przepisami ustawy o ochronie danych osobowych jest przede wszystkim, aby czynność przetwarzania danych osobowych przez ich administratora znajdowała podstawę prawną w jednej z ustawowych przesłanek, określonych w art. 23 ust 1 pkt 1-5 ustawy o ochronie danych osobowych (w odniesieniu do danych

zwykłych, jak np. imię, nazwisko, adres zamieszkania) lub w art. 27 ust. 2 pkt 1-10 ustawy o ochronie danych osobowych (w przypadku przetwarzania danych szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych). Ponadto administrator danych, obowiązany jest również - zgodnie z art. 26 ust. 1 pkt 1-4 ustawy o ochronie danych osobowych - 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 (pkt 1), zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (pkt 2), merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (pkt. 3), oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (pkt 4). Statuowana w art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych zasada legalizmu przewiduje obowiązek przetwarzania danych zgodnie z prawem. Należy przez to rozumieć zgodność nie tylko z przepisami obowiązującej ustawy, ale także wszelkimi obowiązującymi normami prawa, zarówno przepisami prawa materialnego i procesowego, rangi ustawowej czy norm zawartych w aktach wykonawczych. Jednocześnie zasada związania celem, o której stanowi pkt 2 ww. przepisu, obliguje do zbierania danych osobowych tylko dla oznaczonych i zgodnych z prawem celów.

Mając na uwadze uchylenie szczególnych przepisów prawa uprawniających hotele i inne zakłady do gromadzenia danych osób korzystających z ich usług dla celów meldunkowych, Generalny Inspektor Ochrony Danych Osobowych zajął stanowisko, że brak było legalnej przesłanki przetwarzania ww. danych przez te podmioty dla takich celów, a tym samym tworzenia i prowadzenia zbiorów danych w związku z realizacją tych celów. Powstała zatem konieczność ponownej weryfikacji – w oparciu o ten stan prawny – zbiorów prowadzonych (zarejestrowanych bądź zgłoszonych do rejestracji w ogólnopolskim rejestrze zbiorów danych osobowych prowadzonym przez GIODO) przez podmioty dotąd do tego zobowiązane.

Mając na uwadze powyższe, Generalny Inspektor wezwał Polską Izbę Hotelarstwa do zasygnalizowania podmiotom zajmującym się świadczeniem usług hotelarskich, konieczności przestrzegania obowiązujących przepisów prawa.

W odpowiedzi pismami z dnia 3 lipca 2013 i 25 lipca 2013 r. Dyrektor Generalny Polskiej Izby Hotelarstwa poinformował o podjętych działaniach, m.in. o wystąpieniu do marszałków województw w tej sprawie.

Generalny Inspektor Ochrony Danych Osobowych wystąpił w dniu 29 lipca 2013 r. do Ministra Pracy i Polityki Społecznej o rozważenie wprowadzenia w przepisach ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej, zmian w zakresie regulacji dotyczących przetwarzania danych osobowych[381].

W wystąpieniu Generalny Inspektor Ochrony Danych Osobowych wskazał w pierwszej kolejności na zgłaszane przez praktyków realizujących normy ustawy o wspieraniu rodziny i systemie pieczy zastępczej, wątpliwości dotyczące art. 241 ust. 4 ustawy o wspieraniu rodziny i pieczy zastępczej. Zgodnie z brzmieniem tego przepisu, podmiot prowadzący przed dniem wejścia w życie niniejszej ustawy ośrodek adopcyjno-opiekuńczy, w terminie do dnia 15 stycznia 2012 r., przekazuje za zgodą osób zainteresowanych właściwemu: 1) staroście - dokumentację dotyczącą kandydatów do pełnienia funkcji rodziny zastępczej lub prowadzenia placówki rodzinnej oraz rodzin zastępczych i osób prowadzących placówki rodzinne; 2) marszałkowi województwa - dokumentację dotyczącą osób zgłaszających gotowość przysposobienia dziecka oraz prowadzonych procedur przysposobienia. Powyższy przepis jest przepisem przejściowym zobowiązującym podmioty, które wraz z wejściem w życie ustawy utraciły uprawnienie do prowadzenia ośrodka adopcyjnego, do przekazania posiadanej dokumentacji dotyczącej kandydatów do pełnienia funkcji rodziny zastępczej lub prowadzenia placówki rodzinnej oraz rodzin zastępczych i osób prowadzących placówki rodzinne staroście, natomiast - dokumentację dotyczącą osób zgłaszających gotowość przysposobienia dziecka oraz prowadzonych procedur przysposobienia - marszałkowi województwa. Przepis ten uzależnia przekazanie powyższej dokumentacji „od zgody osób zainteresowanych". W ocenie GIODO uzależnienie przekazania dokumentacji od „zgody osób zainteresowanych" jest zbędne i implikuje poważne problemy praktyczne. Przede wszystkim podmioty, do których adresowany jest powyższy przepis sygnalizują organowi ochrony danych osobowych, że w przypadku dokumentów dotyczących zakończonego procesu adopcji nie ma możliwości zwrócenia się do osób, których dane zawarte są w dokumentacji celem uzyskania ich zgody na przekazanie ich dokumentacji ponieważ

[381] DOLiS-035-1996/13

wysłanie korespondencji lub inna próba nawiązania kontaktu z takimi osobami może spowodować ujawnienie faktu adopcji w danej rodzinie (i związane z tym naruszenie tajemnicy adopcji) co z kolei mogłoby skutkować niepowetowanymi stratami w procesie wychowania adoptowanego dziecka.

Ponadto istotne wątpliwości budzi sytuacja, w której podmiot, który utracił uprawnienia do prowadzenia ośrodka adopcyjnego - i jak można wnioskować również do prowadzenia dokumentacji związanej z realizacją tego zadania - musi w dalszym ciągu przechowywać dokumentację, na której przekazanie „osoby zainteresowane" nie wyraziły zgody. Tymczasem dla dopuszczalności przetwarzania danych osobowych lub prowadzenia określonego rodzaju dokumentacji wystarczające jest istnienie stosownego przepisu prawa właściwie wyznaczającego zasady i granice postępowania. Wprowadzanie dodatkowej przesłanki w postaci „zgody" jest zbędne, ponieważ przesłanki legalizujące przetwarzanie danych osobowych mają charakter autonomiczny oraz rozłączny i są co do zasady są równoprawne. Tym samym spełnienie którejkolwiek z nich czyni legalnym proces przetwarzania danych. Przetwarzanie danych osobowych jest dopuszczalne m.in. wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy) albo gdy przepis szczególny innej ustawy zezwala na przetwarzanie danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony (art. 27 ust. 1 pkt 2 ustawy). Mimo upływu wskazanego w tym przepisie terminu na przekazanie dokumentacji, to jest 15 stycznia 2012 r., powyższy problem w wielu przypadkach nie został rozwiązany i wobec tego potrzeba zmiany art. 241 ust. 4 polegająca na usunięciu zbędnego zapisu „za zgodą osób zainteresowanych", była nadal aktualna. Zmiana ta spowoduje wyeliminowanie istniejących wątpliwości, jaki podmiot i w jaki sposób powinien postąpić z dokumentacją, w stosunku do której brak jest zgody lub nawet brak możliwości uzyskania zgody osób zainteresowanych na jej przekazanie.

Istotne wątpliwości wzbudza również art. 46 ust. 2 ustawy, który zawiera katalog danych objętych prowadzonymi przez starostę rejestrami o osobach: 1) zakwalifikowanych do pełnienia funkcji rodziny zastępczej zawodowej, rodziny zastępczej niezawodowej lub do prowadzenia rodzinnego domu dziecka; 2) pełniących funkcję rodziny zastępczej zawodowej lub rodziny zastępczej niezawodowej oraz prowadzących rodzinny dom dziecka. Pośród danych wymienionych w tym przepisie są „dane o stanie zdrowia niezbędne do stwierdzenia, że osoba może sprawować właściwą opiekę nad dzieckiem" (pkt 11). W opinii

Generalnego Inspektora Ochrony Danych Osobowych sformułowanie powyższe jest nieprecyzyjne i stwarza pole do gromadzenia danych w zbyt szerokim, nieadekwatnym do celu zakresie. Rozważenia wymaga, czy przepis ten nie powinien być zmieniony na przykład na następujący zapis: „*informacje o aktualnym zaświadczeniu o braku przeciwwskazań zdrowotnych do pełnienia funkcji rodziny zastępczej, rodziny zastępczej niezawodowej lub do prowadzenia rodzinnego domu dziecka, wystawionymi przez lekarza podstawowej opieki zdrowotnej*". W ten sposób wyeliminowane zostałyby wątpliwości co do zgodności tego przepisu z przepisami o ochronie danych osobowych. Ustawa o ochronie danych osobowych zapewnia specjalny reżim ochrony danym o stanie zdrowia, a więc danym należącym do kategorii „szczególnie chronionych". Zgodnie z art. 27 ustawy przetwarzanie powyższych danych jest co do zasady zabronione. Zasada ta doznaje wyjątków jedynie w przypadkach enumeratywnie wyliczonych w art. 27 ust. 2 ustawy. Przy czym wobec jednoznacznej dyspozycji art. 27 ust. 2 pkt 2 tej ustawy, gdyby podstawę dla przetwarzania danych sensytywnych miał 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 precyzyjnie określać rodzaj i zakres danych uwzględniając cel ich pozyskiwania.

Analogiczne uwagi należy odnieść do art. 160 ust 2 pkt 10 ustawy odnoszącego się do gromadzenia przez ośrodek adopcyjny informacji dotyczących kandydatów do przysposobienia dziecka w postaci danych o stanie zdrowia niezbędnych do stwierdzenia, że osoba może sprawować właściwą opiekę nad dzieckiem.

W odniesieniu do art. 162 i 163 ustawy wskazać należy, że brak jest w niej materialnoprawnych podstaw do prowadzenia „wojewódzkiego banku danych" oraz „centralnego banku danych". Uprawnienie do prowadzenia takich zbiorów danych dla określonych podmiotów, powinno być przewidziane w przepisie rangi ustawowej. W przepisie ustawy powinny być również określone: zasady prowadzenia takich zbiorów, w tym zasady pozyskiwania i udostępniania danych osobowych. Powołane przepisy, jako przepisy stanowiące jedynie o sposobie wyznaczania ośrodków pełniących rolę podmiotów prowadzących takie bazy, nie mogą być uznane za przepisy o takim charakterze. Należy także

wprowadzić przepisy regulujące zakres danych zamieszczanych w takich rejestrach oraz dookreślić zasady przesyłania informacji pomiędzy właściwymi ośrodkami. Jako, iż przedmiotem udostępniania są w tym przypadku także dane o stanie zdrowia należy z rozwagą formułować przepisy umożliwiające wymianę tych danych pomiędzy wszystkimi ośrodkami adopcyjnymi na trenie Rzeczypospolitej Polskiej. Warto zaznaczyć, iż przyznawanie określonym podmiotom uprawnień do przetwarzania danych (ich pozyskiwania i udostępniania), w szczególności tych o charakterze sensytywnym, w każdym przypadku winno być poprzedzone analizą rzeczywistej konieczności władania nimi przez podmioty uprawnione.

W odpowiedzi pismem z dnia 13 sierpnia 2013 r. Minister Pracy i Polityki Społecznej zapewnił, że wskazane w wystąpieniu problemy zostaną poddane dogłębnej analizie podczas prac nad najbliższą nowelizacją ustawy.

Podjęcie prac legislacyjnych mających na celu kompleksowe uregulowanie problematyki dotyczącej przetwarzania danych osobowych przez starostów, którzy dokonują rejestracji pojazdu na gruncie przepisów ustawy z dnia 20 czerwca 1997 r. - **Prawo o ruchu drogowym (Dz. U. z 2012 r. poz. 1137 z późn. zm.), było głównym celem wystąpienia GIODO z dnia 31 lipca 2013 r. do Ministra Transportu, Budownictwa i Gospodarki Morskiej (obecnie Minister Infrastruktury i Rozwoju)** [382]**.**

Stosownie do treści art. 73 ust. 1 ustawy - Prawo o ruchu drogowym, rejestracji pojazdu dokonuje, na wniosek właściciela, starosta właściwy ze względu na miejsce jego zamieszkania (siedzibę), wydając dowód rejestracyjny i zalegalizowane tablice (tablicę) rejestracyjne oraz nalepkę kontrolną, jeżeli jest wymagana, z zastrzeżeniem ust. 2-5. Rejestracja pojazdu dokonywana jest po przedłożeniu odpowiednich dokumentów wymienionych w art. 72 ustawy - Prawo o ruchu drogowym.

Zgodnie z art. 80a ust. 1 i 2 ustawy - Prawo o ruchu drogowym, w centralnej ewidencji pojazdów gromadzi się dane i informacje o pojazdach zarejestrowanych oraz o ich właścicielach lub niektórych posiadaczach. Ewidencję tę prowadzi minister właściwy do spraw wewnętrznych w systemie teleinformatycznym i to ten właśnie organ jest administratorem danych i informacji zgromadzonych w ewidencji (ust. 4 ww. przepisu). Centralna ewidencja prowadzona jest w oparciu o dane przekazane do ewidencji przez organ

[382] DOLiS-035-1996/13

właściwy w sprawach rejestracji pojazdów, a więc właściwego starostę (art. 73 ust. 1 ustawy - Prawo o ruchu drogowym). Zagadnienie dotyczące zakresu uprawnień starosty w zakresie przetwarzania danych osobowych w celu realizacji obowiązków nałożonych ustawą - Prawo o ruchu drogowym, uregulowane zostało przepisami rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 19 września 2001 r. w sprawie centralnej ewidencji pojazdów (Dz. U. Nr 106, poz. 1166 z późn. zm.) oraz rozporządzenia Ministra Infrastruktury z dnia 27 września 2003 r. w sprawie szczegółowych czynności organów w sprawach związanych z dopuszczeniem pojazdu do ruchu oraz wzorów dokumentów w tych sprawach (Dz. U. z 2007 r. Nr 137, poz. 968 z późn. zm.).

Zgodnie z § 4 ust. 1 ww. rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie centralnej ewidencji pojazdów, dane i informacje, o których mowa w art. 80b ust. 1 pkt 1-5 i pkt 6 lit. a i c oraz ust. 1a ustawy, przekazuje do ewidencji, poprzez teletransmisję, organ właściwy w sprawach rejestracji pojazdów, a więc odpowiednio starosta, o którym mowa w art. 73 ust. 1 ustawy - Prawo o ruchu drogowym, niezwłocznie po dokonaniu odpowiednio rejestracji pojazdu, zmiany danych w dowodzie rejestracyjnym albo uzyskaniu informacji o utracie dowodu rejestracyjnego, tablic rejestracyjnych, pozwolenia czasowego, tablic tymczasowych lub karty pojazdu, a także ich odnalezieniu. Natomiast przepisy ww. rozporządzenia Ministra Infrastruktury w sprawie szczegółowych czynności organów w sprawach związanych z dopuszczeniem pojazdu do ruchu oraz wzorów dokumentów w tych sprawach, wskazują wprost na prowadzenie przez organ rejestrujący bazy danych służącej do gromadzenia i przetwarzania danych (§ 1 pkt 7a). Przepis § 3 ust. 1 i 2 omawianego rozporządzenia stanowi, iż organ rejestrujący zamieszcza w ww. bazie danych dane i informacje o pojazdach zarejestrowanych, czasowo zarejestrowanych, wyrejestrowanych oraz ich właścicielach i niektórych posiadaczach z uwzględnieniem danych i informacji, o których mowa w art. 80b ust. 1 i 1a ustawy Prawo o ruchu drogowym, czyniąc to w oparciu o dokumenty wymagane do rejestracji pojazdu zgodnie z przepisami o rejestracji pojazdów. Dane i informacje, o których mowa w art. 80b ust. 1 i 1a ustawy - Prawo o ruchu drogowym, organ rejestrujący przekazuje z bazy danych, zgodnie z ww. ustawą, do ewidencji pojazdów, na zasadach określonych w przepisach wydanych na podstawie art. 80e ust. 1 ww. ustawy, z wykorzystaniem systemu teleinformatycznego rejestracji (§ 3 ust. 3).

Generalny Inspektor Ochrony Danych Osobowych wskazał, że nie ma wątpliwości co do tego, że działalność starosty wiąże się z przetwarzaniem danych osobowych. Starosta jest

administratorem prowadzonych przez siebie zbiorów. Jako organ rejestrujący gromadzi w ramach tych zbiorów dane, które przekazywane są następnie, na podstawie ustawy - Prawo o ruchu drogowym, do zbioru danych (centralnej ewidencji pojazdów), którego administratorem jest minister właściwy do spraw wewnętrznych. Starosta posiada status administratora danych odrębnego od ministra właściwego do spraw administracji w zakresie prowadzonego przez siebie zbioru danych i informacji. Istotne wątpliwości natomiast, z punktu widzenia zasad przetwarzania danych osobowych określonych w ustawie o ochronie danych osobowych, wzbudza brak szczegółowych regulacji dotyczących zasad i sposobu udostępniania danych ze zbiorów prowadzonych przez starostę na podstawie ustawy - Prawo o ruchu drogowym. W związku z tym, że przepisy tej ustawy nie regulują szczegółowych zasad udostępniania danych z posiadanej przez starostę dokumentacji, powstają istotne wątpliwości, komu i w jaki sposób dokumentacja określona w art. 80b ust. 1 i 1a ustawy - Prawo o ruchu drogowym, w tym dane o właścicielu pojazdu oraz o posiadaczu tego środka transportu, ma być udostępniana.

Generalny Inspektor zauważył, że w odniesieniu do centralnych ewidencji prowadzonych przez ministra właściwego do spraw wewnętrznych, znacznie szersze uregulowania w zakresie zasad udostępniania danych z tych ewidencji zawierają przepisy art. 80c ustawy - Prawo o ruchu drogowym, dotyczące centralnej ewidencji pojazdów oraz art. 100c ww. ustawy odnoszące się do centralnej ewidencji kierowców. Przepisy te w sposób szczegółowy określają kategorie podmiotów uprawnionych oraz sposób i zakres udostępniania im danych zgromadzonych w centralnej ewidencji.

Wyżej wymienione przepisy określają w sposób wyraźny kompetencje właściwego ministra podejmującego procedurę zmierzającą do udostępnienia danych zgromadzonych w centralnych ewidencjach. Określone podmioty kwalifikowane są do występowania z wnioskiem o udostępnienie danych zawartych w ww. rejestrach, i tylko tym podmiotom przepisy prawa nadają uprawnienie do pozyskania informacji o osobie, której procedura ewidencjonowania dotyczy. Rygorom udostępniania danych nie został zaś objęty starosta, który jest organem właściwym dla podejmowania procedury rejestracji pojazdu. Jak wyżej zauważono, starosta staje się jednak i tak dysponentem takich danych we wcześniejszym etapie, skoro pozyskuje informacje o osobach. W ten sposób naruszane są konstytucyjnie gwarantowane prawa osób, których przedmiotowa dokumentacja dotyczy. Konstytucja RP stanowi bowiem, że każdy ma prawo dostępu do dotyczących go urzędowych dokumentów

i zbiorów danych. Ograniczenie tego prawa może określić jedynie ustawa (art. 51 ust. 3 Konstytucji RP).

Z tego względu Generalny Inspektor poddał pod rozwagę sposób rozwiązania istniejącego problemu, w drodze odpowiedniej nowelizacji ustawy - Prawo o ruchu drogowym, zmierzającej do wyczerpującego uregulowania kwestii udostępniania danych osobowych przetwarzanych przez starostę w związku z dokonywaniem rejestracji pojazdu. W przedmiotowej bowiem sprawie istniejące normy kompetencyjne wydają się nie uwzględniać w pełni interesu obywateli. Z jednej strony brak przepisów regulujących kwestie związane z udostępnianiem danych zgromadzonych przez starostę w wyniku prowadzenia procedury rejestracji pojazdu, skutkuje powstaniem luki prawnej w tym zakresie, z drugiej zaś strony przyjęcie rozwiązania powierzającego starostom przetwarzanie danych osobowych może prowadzić do nieograniczonej ramami prawnymi uznaniowości co do kwalifikacji podmiotu, któremu dane te można udostępnić, jak również sposobu i zakresu ich udostępnienia. Skutkiem braku wyczerpującego uregulowania kwestii, które odnoszą się do przedmiotowego zagadnienia jest pozostawienie staroście decyzji co do sposobu postępowania w kwestii udostępniania danych zgromadzonych przed tym organem w wyniku prowadzenia procedury rejestracji pojazdu.

Należy także podkreślić, iż stosownie do treści art. 7 Konstytucji Rzeczypospolitej Polskiej, organy władzy publicznej działają na podstawie i w granicach prawa. Zasada ta nakazuje, by wszelkie działania organów władzy publicznej były oparte na wyraźnie określonych normach kompetencyjnych. Natomiast obowiązujące postanowienia w tym zakresie budzą jednak wątpliwości co do wypełnienia przez nie ww. wymogów przejrzystości norm prawa.

Generalny Inspektor uznał zatem za konieczne podjęcie prac legislacyjnych w celu precyzyjnego uregulowania zasad udostępniania danych osobowych, które przetwarza starosta w procesie dokonywania rejestracji pojazdów, w szczególności określenia wprost kategorii podmiotów, które mogłyby występować z wnioskiem o ich udostępnienie oraz zakresu i sposobu tego udostępnienia. Wzór dla stosownych zmian w omawianym zakresie mogłyby stanowić odpowiednie regulacje dotyczące udostępniania danych zgromadzonych w centralnych ewidencjach, w tym centralnej ewidencji pojazdów, w szczególności w art. 80c ustawy - Prawo o ruchu drogowym.

W odpowiedzi pismem z dnia 11 września 2013 r. Minister Transportu, Budownictwa i Gospodarki Morskiej (obecnie Minister Infrastruktury i Rozwoju) poinformował, że konsultował przedstawione zagadnienie z Ministrem Spraw Wewnętrznych, który poinformował m.in. że udostępnianie danych i informacji z Centralnej Ewidencji Pojazdów lub Centralnej Ewidencji Kierowców zostało wystarczająco uregulowane w ustawie – Prawo o ruchu drogowym, natomiast do udostępniania danych przez starostę zastosowanie znajdują przepisy ustawy o ochronie danych osobowych. Stanowisko to podziela Minister Infrastruktury i Rozwoju stwierdzając, że nie ma konieczności podjęcia prac nad nowelizacją przepisów Prawa o ruchu drogowym.

Pismem z dnia 4 grudnia 2013 r. Generalny Inspektor Ochrony Danych Osobowych podziękował za przedstawione wątpliwości w sprawie, wskazując i dodatkowo argumentując swoje zastrzeżenia. W ocenie organu jego wystąpienie warte jest ponownego przeanalizowania. Przedmiotowe zagadnienie jest bowiem niezwykle istotne z punktu widzenia problematyki dotyczącej przetwarzania danych osobowych i ich ochrony.

Wobec powyższego, pismem z dnia 10 stycznia 2014 r. Minister Infrastruktury i Rozwoju poinformował, że przedstawione przez Generalnego Inspektora zagadnienie będzie przedmiotem dalszej analizy oraz konsultacji z Ministrem Spraw Wewnętrznych. Ministerstwo Infrastruktury i Rozwoju rozważy również zasięgnięcie w tej sprawie opinii strony samorządowej, a stanowisko Ministra Infrastruktury i Rozwoju zostanie przedstawione w terminie późniejszym.

Z kolei wystąpienie GIODO z dnia 6 sierpnia 2014 r. dotyczyło wprowadzenia odpowiednich procedur gwarantujących przestrzeganie prawa do prywatności osób objętych monitoringiem wizyjnym[383].

Impulsem do tego wystąpienia stała się skarga pracowników dotycząca przetwarzania przez spółkę ich danych osobowych w zakresie wizerunku, przy wykorzystaniu systemu monitoringu wizyjnego zainstalowanego w szatni oraz rejestracji dźwięku. Osoby skarżące przyznały, iż zostały poinformowane ustnie o rejestracji wizji za pomocą stosowanego przez spółkę monitoringu, natomiast co do rejestracji dźwięku za pomocą ww. urządzenia – w sprawie brak było dostatecznych dowodów na to, by spółka dopełniła obowiązku informacyjnego również i w tym zakresie.

[383] Pismo GIODO z dnia 6 sierpnia 2013 r. (DOLiS-440-389/12/AZ/I/49938)

GIODO zwrócił uwagę na przyjętą w dniu 11 lutego 2004 r. opinię Nr 4/2004 Grupy Roboczej do spraw ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołanej na podstawie art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych – GR Art. 29 (Dz.U.UE.L.95.281.31). W opinii tej zwrócono uwagę m.in. na konieczność respektowania zasady proporcjonalności przy posługiwaniu się wideonadzorem, która oznacza przede wszystkim, że urządzenia monitoringu mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony i/lub bezpieczeństwa, o charakterze fizycznym i/lub logicznym, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami. Ta sama zasada dotyczy również wyboru odpowiedniej technologii, kryteriów wykorzystywania urządzeń w konkretnych sytuacjach oraz ustaleń dotyczących przetwarzania danych, odnoszących się także do zasad dostępu i okresu przechowywania. Istotne znaczenie ma w tej materii – jak dalej traktuje ww. opinia – realizacja obowiązku informacyjnego wobec osób, których dane osobowe pozyskane zostały za pomocą monitoringu, zgodnie z wymogami art. 10 i 11 ww. Dyrektywy 95/46/WE. Wskazano przy tym, iż osoby te muszą mieć świadomość faktu prowadzenia czynności monitorujących, tablice informacyjne o wideonadzorze powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc oraz posiadać wymiary proporcjonalne do miejsca, gdzie są umieszczone. Muszą także wskazywać cele działań nadzoru, jak również administratora przetwarzania. Mając powyższe na uwadze GIODO zwrócił o wprowadzenie odpowiednich procedur związanych z przedmiotowym monitoringiem w zakresie rejestracji wizji i fonii, uwzględniającym powyższe wytyczne i gwarantującym przestrzeganie prawa do prywatności osób nim objętych.

W odpowiedzi na wystąpienie spółka wskazała, iż w widocznym miejscu umieszczona została tablica informująca o stosowanym w obiekcie monitoringu, pracownicy zostali poinformowani o zainstalowanym urządzeniu monitoringu wraz ze wskazaniem miejsc rejestracji. Ponadto wszyscy pracownicy sporządzili stosowne oświadczenia, w których potwierdzili, iż zostali poinformowani o zamontowanych urządzeniach monitorujących,

zostali zapoznani ze sposobem i celem działania urządzeń, jak i faktem administrowania przez spółkę danymi w formie zapisu z urządzenia.

Przedmiotem wystąpienia z dnia 3 września 2013 r. do jednego z zakładów karnych było podjęcie działań, mających na celu dostosowanie procesu przechowywania i przetwarzania przez ten podmiot danych osobowych osób w nim osadzonych do wymogów określonych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)[384].

Generalny Inspektor Ochrony Danych Osobowych uzyskał informacje o szeregu zdarzeniach w jednym z zakładów karnych, w wyniku których zostały udostępnione, bądź też niewłaściwie zabezpieczone, dane osobowe, w tym dane sensytywne, które w rozumieniu art. 27 ustawy o ochronie danych osobowych podlegają szczególnej ochronie. Generalny Inspektor został poinformowany, że w ogólnodostępnym koszu na śmieci znajdowały się m.in. dokumenty z danymi osób konwojowanych oraz zawierające szereg informacji dotyczących konwoju. Ponadto osobom postronnym dostępne były również inne dane osobowe, w tym dotyczące danych księgowych zawartych na listach sald, jak również dane adresatów i nadawców przesyłek dla więźniów.

Przedstawiony stan rzeczy budził poważne wątpliwości pod kątem ich zgodności z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Konstytucji RP (art. 47), ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz. U. Nr 90, poz. 557 z późn. zm.) oraz m.in. rozporządzenia Ministra Sprawiedliwości z dnia 25 sierpnia 2003 r. w sprawie regulaminu organizacyjno – porządkowego wykonywania kary pozbawienia wolności (Dz. U. Nr 152, poz. 1493). Przy czym zastrzec należy, że postanowienia regulaminu, jako aktu o charakterze wewnętrznym obowiązującym w ramach danej jednostki, muszą odpowiadać normom wyższego rzędu, w tym wynikającym z powszechnie obowiązujących przepisów prawa. W tym zakresie należy uwzględnić art. 24 ust. 1 tej ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej (Dz. U. Nr 79, poz. 523 z późn. zm.), który odwołując się do art. 2 ust. 2 pkt 3 powołanej ustawy zobowiązuje - w zakresie przetwarzania danych osobowych - do zapewnienia osobom skazanym na karę pozbawienia wolności lub tymczasowo aresztowanym, a także osobom, wobec których są wykonywane kary pozbawienia wolności i środki przymusu skutkujące pozbawieniem wolności, przestrzegania

[384] DOLiS-2245/13

ich praw, a zwłaszcza humanitarnych warunków bytowych, poszanowania godności, opieki zdrowotnej i religijnej. Uwzględniając specyfikę jednostek izolacyjnych należy zauważyć, że kwestionowana praktyka przyczyniła się do dotkliwego dla osadzonych poczucia braku bezpieczeństwa w sytuacji, gdy inne osoby przebywające w zakładzie karnym mogły z łatwością pozyskać ich dane osobowe udostępnione na przesyłkach - na których widniały też dane osobowe nadawcy - oraz zasięgnąć informacji na temat danych osobowych osób konwojowanych. Dane te bowiem znajdowały się w miejscach, do których miały lub mogły mieć dostęp osoby nieupoważnione do ich przetwarzania. Administrator danych winien przestrzegać przepisów rozdziału 5 ustawy o ochronie danych osobowych, a w konsekwencji tak zorganizować proces przetwarzania danych osobowych, którymi dysponuje, aby uczynić zadość spoczywającemu na nim obowiązkowi prawidłowego zabezpieczenia tych danych przed ich udostępnieniem osobom nieuprawnionym. Przepisy prawa wymagają zatem od Służby Więziennej dołożenia wszelkich starań, aby dane osobowe znajdujące się na dokumentach konwojowych były odpowiednio zabezpieczone przed nieuprawnionym dostępem osób niepowołanych. To samo dotyczy przetwarzania innych danych osobowych, ponieważ udostępnianie takich danych osobom nieupoważnionym jest niedopuszczalne i stanowi naruszenie konstytucyjnie gwarantowanego prawa do prywatności.

W odpowiedzi Dyrektor Zakładu Karnego poinformował o wprowadzeniu procedur mających na celu zapobieganie udostępnianiu danych osobowych osobom nieupoważnionym.

Z kolei wystąpienie z dnia 6 listopada 2012 r. związane było z udostępnieniem na stronie internetowej Ministerstwa Edukacji Narodowej danych osobowych ekspertów MEN, które w opinii GIODO nastąpiło bez podstawy prawnej[385].

Generalny Inspektor zwrócił się do Minister Edukacji o: 1) podjęcie działań, mających na celu dostosowanie procesu przetwarzania danych osobowych przez Ministerstwo Edukacji Narodowej w zakresie udostępnionych na stronach internetowych danych ekspertów do wymogów określonych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.); 2) podjęcie prac legislacyjnych mających na celu kompleksowe uregulowanie kwestii związanych z przetwarzaniem danych osobowych określonych w rozporządzeniu z dn. 1 marca 2013 roku (Dz. U. z 2013 r. poz. 354). Wystąpienie spowodowane było pozyskaniem przez Generalnego Inspektora Ochrony

[385] DOLiS-035-3533/13

Danych Osobowych informacji o publikowaniu na stronie internetowej Ministerstwa Edukacji Narodowej list z danymi osobowymi ekspertów wchodzących w skład komisji egzaminacyjnych i kwalifikacyjnych. Dane te, dotyczące ekspertów z całej Polski, są powszechnie dostępne na stronie internetowej MEN. Zakres udostępnionych danych obejmuje: imię i nazwisko, kwalifikacje zawodowe, zajmowane stanowisko, adres, numer telefonu (stacjonarnego lub komórkowego) oraz adres e-mail.

Powyższy stan rzeczy budził poważne wątpliwości pod kątem zgodności z przepisami ustawy o ochronie danych osobowych i konstytucyjnie gwarantowanego prawa do prywatności. GIODO wskazał, że zgodnie z art. 23 ustęp 1 ww. ustawy, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela (Dz. U. z 2006 r. Nr 97 poz. 674 z późn. zm.) stanowi, iż w skład komisji egzaminacyjnych dla nauczycieli ubiegających się o awans na stopień nauczyciela mianowanego, a także dyplomowanego wchodzą eksperci z listy ustalonej przez ministra właściwego do spraw oświaty i wychowania (art. 9g ustęp 2 pkt 4 i art. 9g ustęp 3 pkt. 3). Listę ekspertów prowadzi minister właściwy do spraw oświaty i wychowania (art. 9g ustęp 11). Zgodnie z art. 9g ustęp 11d wpis na listę ekspertów, odmowa wpisu oraz skreślenie następuje w drodze decyzji administracyjnej ministra właściwego do spraw oświaty i wychowania. Art. 9g ust. 12 stanowi z kolei, że minister właściwy do spraw oświaty i wychowania określi, w porozumieniu z ministrem właściwym do spraw kultury i ochrony dziedzictwa narodowego, Ministrem Obrony Narodowej i Ministrem Sprawiedliwości, w drodze rozporządzenia, ramowy program szkolenia kandydatów na ekspertów, sposób prowadzenia listy ekspertów, tryb wpisywania i skreślania ekspertów z listy, uwzględniając w szczególności podstawowe treści programowe szkolenia i minimalny wymiar godzin szkolenia, a także dokumenty wymagane od osób ubiegających się o wpis na

listę ekspertów oraz zakres danych objętych wpisem na listę. Dyspozycję tę wypełnia rozporządzenie Ministra Edukacji Narodowej z dnia 1 marca 2013 r. w sprawie ramowego programu szkolenia kandydatów na ekspertów wchodzących w skład komisji egzaminacyjnych i kwalifikacyjnych dla nauczycieli ubiegających się o awans na stopień zawodowy, sposobu prowadzenia listy ekspertów oraz trybu wpisywania i skreślania ekspertów z listy (Dz. U. z 2013 r. poz. 354). Rozporządzenie to nie było konsultowane z Generalnym Inspektorem Ochrony Danych Osobowych na etapie uzgadniania postanowień wynikających z jego przepisów.

Tymczasem w opinii Generalnego Inspektora Ochrony Danych Osobowych wątpliwość budził w pierwszej kolejności § 3 ust. 3 pkt 9 w/w rozporządzenia, zgodnie z którym do wniosku o wpis na listę ekspertów należy dołączyć oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, w celu związanym z prowadzeniem listy ekspertów, zgodnie z ustawą o ochronie danych osobowych. Należy zauważyć, że instytucja zgody w tym przypadku nie powinna mieć zastosowania, gdyż przesłanką legalizującą przetwarzanie danych dla określonych mocą rozporządzenia potrzeb, w tym prowadzenia listy ekspertów powinien być i jest przepis prawa (art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych). Wymaganie zgody na przetwarzanie danych osobowych od ekspertów, których listę prowadzi minister właściwy do spraw oświaty i wychowania budzi wątpliwości chociażby z tego powodu, że zgoda taka jest *de facto* wymuszona, z drugiej strony jest zbędna, innymi słowy nie musi, a wręcz nie powinna być pozyskiwana skoro dane przetwarzane są na podstawie stosownych przepisów rozporządzenia. Należy uznać, że ze zgodą w rozumieniu ustawy o ochronie danych osobowych można mieć do czynienia wyłącznie, gdy dana osoba ma możliwość wyznaczenia zakresu udostępnianych danych oraz cofnięcia tej zgody w dowolnym momencie. Warto w tym miejscu odnotować, że w świetle orzecznictwa, zgoda na przetwarzanie danych osobowych nie ma wpływu na uprawniania danego eksperta. Takie stanowisko zaprezentował Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 1 lutego 2005 r. sygn. II SA/Wa 1294/04: *„Brak pisemnego oświadczenia eksperta o wyrażeniu zgody na przetwarzanie jego danych osobowych pozostaje bez wpływu na prawidłowość powołania komisji kwalifikacyjnej”*[386].

[386] LEX nr 165761

Niezależnie od powyższego uznać należało, że udostępnienie list ekspertów na stronie internetowej Ministerstwa Edukacji Narodowej oparte było na wątpliwej podstawie prawnej, którą można by zastosować wyłącznie w przypadku, gdy dana osoba miałaby możliwość decydowania o tym, czy udostępnić (a jeśli tak to w jakim zakresie) dane osobowe. Powyższe nie ma zastosowania, gdy przesłanką legalizującą stanowi przepis prawa. Ponadto § 7 Rozporządzenia Ministra Edukacji Narodowej z dn. 1 marca 2013 r., o którym była mowa wyżej, stanowi jedynie, iż lista ekspertów jest prowadzona w formie elektronicznej bazy danych, nie ma natomiast nigdzie mowy o jej udostępnianiu w Internecie. Tak dalece idące naruszenie prywatności bezwzględnie powinno znajdować swoje uzasadnienie w obowiązującym przepisie prawa i wynikać z aktu prawnego rangi ustawowej. W takim przypadku trzeba mieć szczególnie na uwadze, aby zachowana została zasada adekwatności, tj. aby udostępniane były jedynie dane w zakresie niezbędnym do osiągnięcia zamierzonego celu. Każdy administrator danych musi zapewnić, aby dane osobowe były przetwarzane w oparciu o jedną z przesłanek wskazanych w art. 23 ust. 1 – 5 ustawy o ochronie danych osobowych (zasada legalizmu) oraz, aby dane te były przetwarzane w zakresie proporcjonalnym, adekwatnym odpowiednim do celu przetwarzania, stosownie do art. 26 ust. 1 pkt 3 ustawy (zasada adekwatności). Zgodnie z zasadą adekwatności, administrator danych powinien przetwarzać wyłącznie te dane, które są niezbędne ze względu na cel zbierania danych. Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy dobrem osoby, której dane dotyczą a interesem administratora danych. Oznacza to, że 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.

Ponadto rozporządzenie powinno być aktem wykonawczym, a nie prawotwórczym i powinno jedynie precyzować materię określoną w delegacji ustawowej, tzn. powinno dążyć się docelowo do tego, aby zakres danych osobowych, które obejmuje wpis na listę o udostępnieniu ekspertów został umieszczony w akcie o randze ustawy, a ewentualne rozporządzenie powinno zachować wyłącznie wykonawczy charakter. Powyższy postulat powinien być bezwzględnie przestrzegany w przypadku tzw. danych wrażliwych, określonych w art. 27 ust. 1 ustawy o ochronie danych osobowych. Rozporządzenie nie powinno obligować do podawania danych których posiadanie nie jest obowiązkowe. Żaden przepis prawa nie stanowi bowiem, że istnieje obowiązek posiadania numeru telefonu bądź adresu e-

mail. W odpowiedzi na wystąpienie MEN poinformowało, że dane ekspertów są obecnie udostępniane jedynie podmiotom wykonującym ustawową kompetencję powoływania komisji kwalifikacyjnych bądź egzaminacyjnych dla nauczycieli ubiegających się o stopień awansu zawodowego. Dostęp do listy exportu możliwy jest wyłącznie poprzez portal Systemu Informacji Oświatowej, dla użytkowników posiadających login i hasło (w tzw. strefie dla zalogowanych). W ten sposób lista została usunięta z ogólnodostępnych stron internetowych.

Kolejne prezentowane **wystąpienie - z dnia 6 listopada 2013 r. - dotyczyło podjęcia prac legislacyjnych mających na celu doprecyzowanie § 8 ust. 1 rozporządzenia Ministra Sprawiedliwości z dnia 24 stycznia 2005 r. w sprawie biegłych sądowych (Dz. U. z Nr 15 poz. 133) poprzez określenie rodzaju adresu biegłego sądowego zamieszczanego w wykazach i listach prowadzonych przez prezesów sądów, w sposób uniemożliwiający podawanie do publicznej wiadomości informacji obejmujących prywatną sferę życia biegłego sądowego[387].**

W minionym okresie sprawozdawczym organowi do spraw ochrony danych osobowych sygnalizowane były wątpliwości i zastrzeżenia w kwestii dotyczącej ujawniania adresów zamieszkania biegłych sądowych, poprzez ich zamieszczanie na listach biegłych sądowych prowadzonych przez prezesów sądów. Wątpliwości te uzasadniane były przede wszystkim ochroną prywatności osoby wykonującej funkcję biegłego, zbędnością tej informacji do celu jakiemu listy biegłych służą, a także zagrożeniem dla życia prywatnego biegłego sądowego.

Stosownie do brzmienia przepisów rozporządzenia Ministra Sprawiedliwości z dnia 24 stycznia 2005 r. w sprawie biegłych sądowych (Dz. U. z Nr 15 poz. 133), prezes sądu prowadzi listy biegłych sądowych - według poszczególnych gałęzi nauki, techniki, sztuki, rzemiosła, a także innych umiejętności. Prezes prowadzi również wykazy biegłych sądowych na kartach założonych dla każdego biegłego; w listach i wykazach podaje się adres biegłego i termin, do którego został ustanowiony, a także inne dane dotyczące specjalizacji (§ 8 ust. 1). Stosownie do § 8 ust. 3 listy biegłych sądowych są dostępne dla zainteresowanych w sekretariatach sądowych. W szczególności listy te udostępnia się stronom, uczestnikom postępowania oraz organom prowadzącym postępowanie przygotowawcze w sprawach karnych i sądom wojskowym. Wskazany powyżej przepis, który wskazuje jedynie na adres

[387] DOLiS-035-3530-13

biegłego sądowego, skutkuje często upublicznianiem informacji należących do prywatnej sfery życia biegłych sądowych, tj. ich adresów zamieszkania.

Brak dookreślenia, jakiego rodzaju adres biegłego sądowego jest zamieszczany na listach i wykazach upublicznionych w sekretariatach sadowych, rodzi wątpliwości interpretacyjne i może prowadzić do błędnego wniosku, iż niezbędnym jest upublicznianie danych niezwiązanych z życiem zawodowym biegłego, jakimi są informacje o jego adresie zamieszkania – gdy adres ten nie jest jednocześnie miejscem wykonywania określonej działalności zawodowej. Oczywistym pozostaje natomiast, iż w przypadku publikowania informacji o osobie w kontekście sprawowania przez nią pewnej funkcji czy wykonywania działalności, publikacją winny zostać objęte jedynie informacje identyfikujące tę osobę w życiu zawodowym. W analizowanym przypadku należałoby precyzyjnie określić w przedmiotowym rozporządzeniu rodzaj zamieszczanego w listach i wykazach adresu, np. dookreślając, iż jest to adres prowadzonej działalności gospodarczej (zawodowej), adres miejsca zatrudnienia biegłego, czy adres do korespondencji. Należy podkreślić, iż z punktu widzenia przepisów ustawy o ochronie danych osobowych istotne pozostaje, aby administrator danych stosował w procesie przetwarzania danych m.in. zasady celowości i adekwatności, wynikające z art. 26 ust. 1 pkt 2 i 3 ustawy. Dane osobowe swym zakresem i swą treścią nie powinny bowiem wykraczać poza potrzeby wynikające z celu ich przetwarzania (gromadzenia, ujawniania). Administrator danych może zatem przetwarzać wyłącznie takie dane, które są niezbędne do osiągnięcia określonego celu. Upublicznianie danych nieistotnych (danych dotyczących prywatnej sfery życia biegłego sądowego) w stosunku do celu, dla którego są przetwarzane, skutkuje naruszeniem wspomnianej zasady i pozostaje w jaskrawej sprzeczności z przepisami gwarantującymi każdemu prawo do ochrony dotyczących go danych osobowych (art. 1 ust. 1 ustawy o ochronie danych osobowych stanowiącej wykonanie delegacji zawartej w art. 51 ust. 5 Konstytucji RP). Powyższe nabiera znaczenia tym bardziej, gdy wziąć pod uwagę, iż biegli sądowi nierzadko wydają opinię w sprawach, w których podawanie do publicznej wiadomości adresów zamieszkania tychże biegłych może skutkować zagrożeniem dla ich życia prywatnego. Jako przykład przepisów określających precyzyjnie zakres publikowanych danych osobowych biegłych należy wskazać przepisy rozporządzenia Ministra Zdrowia z dnia 27 grudnia 2007 r. w sprawie biegłych w przedmiocie uzależnienia od alkoholu (Dz. U. Nr 250, poz. 1883 z późn. zm.). I tak, § 3 ust. 2a tego rozporządzenia stanowi, iż lista biegłych zawiera

następujące dane: 1) nazwisko i imię; 2) zakres specjalizacji; 3) miejsce i adres zatrudnienia; 4) adres do korespondencji; 5) termin, do którego biegły został powołany. Na marginesie można wskazać, iż także z § 132 w zw. z § 25 ust. 1 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. Nr 100, poz. 908), wynika, iż przepis prawa materialnego powinien możliwie bezpośrednio i wyraźnie wskazywać kto, w jakich okolicznościach i jak powinien się zachować (przepis podstawowy).

Minister Sprawiedliwości w odpowiedzi poinformował, że – z uwagi na sygnalizowane resortowi wątpliwości, dotyczące zakresu dopuszczalnego przetwarzania danych osobowych biegłych sądowych oraz konieczność usprawnienia procesu wyszukiwania biegłych – w Ministerstwie Sprawiedliwości prowadzone są prace legislacyjne, mające na celu nowe ukształtowanie zasad prowadzenia listy biegłych sądowych. Projektowana nowelizacja ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych, przewiduje utworzenie centralnego wykazu biegłych sądowych, prowadzonego w systemie teleinformatycznym administrowanym przez Ministra Sprawiedliwości, a także upoważnienie dla Ministra Sprawiedliwości do określenia – w drodze rozporządzenia – rodzaju informacji przechowywanych w wykazie, zasad i trybu ich udostępniania oraz podmiotów uprawnionych do uzyskania informacji z tego wykazu.

Kolejne prezentowane wystąpienie **(z dnia 8 listopada 2013 r.) skierowane było do Prezesa Zarządu jednej ze spółek o zagwarantowanie przestrzegania wymogów przewidzianych w art. 31 i 37 ustawy o ochronie danych osobowych w wypadku powierzania przetwarzania danych osobowych na rzecz podmiotów trzecich[388].**

Impulsem do niniejszego wystąpienia stała się skarga na przetwarzanie danych osobowych przez spółkę, będącą pracodawcą skarżącego, oraz na przedsiębiorcę świadczącego usługi na rzecz tej półki. Skarżący w szczególności zakwestionował przetwarzanie jego danych osobowych, w tym informacji o przebywaniu przez niego na zwolnieniu lekarskim, przez przedsiębiorcę, który miał na rzecz spółki dokonywać „weryfikacji i zarządzania problemem absencji chorobowej pracowników".

W toku postępowania przeprowadzonego w niniejszej sprawie Generalny Inspektor ustalił, iż spółka i przedsiębiorca zawarli umowę, której przedmiotem było zlecenie

[388] Wystąpienie GIODO z dnia 8 listopada 2013 r. DOLiS-440-1455/12/AZ/I/74083.

przeprowadzenia przez przedsiębiorcę kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich. Ponadto spółka upoważniła przedsiębiorcę do przetwarzania danych osobowych swoich pracowników w celu zrealizowania usługi weryfikacyjnej przedłożonych zwolnień chorobowych w trybie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), a także na podstawie art. 68 ust. 2 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 2010 r. Nr 77, poz. 512 z późn. zm.), do przeprowadzenia kontroli prawidłowości wykorzystywania przez ubezpieczonych zwolnień lekarskich od pracy.

W ocenie GIODO ww. umowa nie spełniała wymogów określonych w art. 31 ust. 1 ustawy, podobnie jak „Upoważnienie do przetwarzania danych osobowych pracowników firmy w celu weryfikacji zwolnień chorobowych", które nie spełniało wymogów przewidzianych art. 37 ustawy. Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Zgodnie natomiast z art. 31 ust. 2 ustawy, podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Dlatego też podmiot przyjmujący od administratora zlecenie przetwarzania danych może je realizować wyłącznie w przewidzianym umową zakresie (chodzi tu głównie o rodzaj danych) oraz w określonym umowie celu (chodzi tu głównie o przeznaczenie danych). Z powyższego wynika zatem, iż ww. umowa powinna zawierać wprost przepisy dotyczące powierzenia ww. danych na rzecz przedsiębiorcy w celu kontroli prawidłowości wykorzystywania przez ubezpieczonych pracowników zwolnień lekarskich od pracy, w tym przede wszystkim dokładny zakres powierzonych danych, tj. wskazanie jakie konkretnie kategorie (rodzaj) danych, spółka powierzyła przedsiębiorcy. Jednocześnie organ do spraw ochrony danych osobowych zwrócił uwagę, iż w przypadku powierzenia danych osobowych na rzecz podmiotu prawa gospodarczego samo nadanie upoważnienia było niewystarczające. Upoważnienie do przetwarzania danych jest bowiem instrumentem związanym z przetwarzaniem danych osobowych przez osoby fizyczne. Natomiast gdy dochodzi do powierzenia danych osobowych do przetwarzania na rzecz innego podmiotu, konieczne było zawarcie przez administratora danych osobowych z tym podmiotem umowy, o której mowa w art. 31 ustawy i dodatkowe nadanie ww. upoważnień. Ponadto podkreślone zostało, iż upoważnienie, o którym mowa w art. 37 ustawy powinno określać dozwolony zakres

przetwarzania danych. Natomiast wobec brzmienia art. 39 ust. 2 ustawy, nadanie upoważnienia powinno być związane z podpisaniem przez osobę obierającą upoważnienie oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz o przyjęciu do wiadomości obowiązku zachowania tajemnicy, czego w niniejszej sprawie zabrakło.

W odpowiedzi na wystąpienie spółka wskazała, iż przedsięwzięła niezbędne działania mające na celu zagwarantowanie przestrzegania wymogów przewidzianych w art. 31 i art. 37 ustawy o ochronie danych osobowych. Ponadto radca prawny spółki został uczulony, aby przy każdej zawieranej umowie weryfikowano, czy przedmiot danego stosunku prawnego łączącego spółkę z osobą trzecią nie pozostaje w związku z ustawą o ochronie danych osobowych.

W związku z informacją o stosowaniu przez Samorządowe Kolegium Odwoławcze formularza wniosku o udostępnienie informacji publicznej, w którym wymagane jest podanie adresu, numeru PESEL i numeru telefonu wnioskodawcy pomimo, iż wnioskodawca ma możliwość otrzymania odpowiedzi na adres poczty elektronicznej, oraz udzielanie zgody na przetwarzanie danych w celu realizacji przedmiotowego wniosku, Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu z dnia 20 listopada 2013 r. zwrócił się o zmianę formularza w celu dostosowania go do przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2001, Nr 112, poz. 1198 z późn. zm.)[389].

W powyższym wystąpieniu Generalny Inspektor powołał się na zasadę legalizmu, zgodnie z którą podmioty publiczne działać mogą jedynie na podstawie i w granicach obowiązujących je przepisów prawa, w ramach kompetencji nadanych im tymi przepisami (art. 7 ustawy z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej - Dz. U. Nr 78, poz. 483, art. 6 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego - Dz. U. z 2013 r. poz. 267 z późn. zm.). W przypadku podmiotów publicznych zarówno zakres, jak i cel przetwarzania danych osobowych jest najczęściej wyznaczony przepisami prawa i wynika on bezpośrednio z określonych prawem zadań danego podmiotu, co determinuje konieczność przyjmowania rozwiązań pozostających w granicach przepisów

[389] DOLiS-035-3675/13

prawa, zarówno jeśli chodzi o zakres i sposób przetwarzania danych jak i zakres zadań, dla realizacji, których dane mają być przetwarzane. Każda z form przetwarzania danych, w tym żądania ich udostępnienia administratorowi danych musi zatem znaleźć oparcie w przepisach prawa. Ustawa o dostępie do informacji publicznej konkretyzuje wyrażone w art. 61 Konstytucji RP ogólne zasady korzystania z prawa do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne poprzez określenie zasad i trybu udostępniania informacji publicznej oraz wskazanie właściwych w tym zakresie organów.

Odnosząc się do norm ogólnych wynikających z ustawy o ochronie danych osobowych GIODO podniósł, że legalność przetwarzania, w tym udostępniania danych osobowych tzw. zwykłych (jak np. imię, nazwisko, adres zamieszkania) uzależniona jest od spełnienia jednej z przesłanek wymienionych w art. 23 ust. 1 pkt 1-5 ustawy o ochronie danych osobowych[390]. Przesłanki legalizujące przetwarzanie danych osobowych mają charakter autonomiczny oraz rozłączny i co do zasady są równoprawne, dlatego też spełnienie jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych. Z punktu widzenia przepisów ustawy o ochronie danych osobowych przetwarzanie danych osobowych jest zatem dopuszczalne m.in. wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy). Tym samym ustawa o ochronie danych osobowych odsyła do przepisów szczególnych, regulujących działalność określonych podmiotów i instytucji, wskazujących w jakich przypadkach i w jakim zakresie mogą one przetwarzać dane osobowe, aby obowiązki i uprawnienia nałożone na nie mocą tych przepisów mogły być realizowane. Stosownie do art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszym akcie prawa. Stosownie do art. 10 ust. 1 ustawy o

[390] Mocą tego przepisu, przetwarzanie danych osobowych „zwykłych" (tj. dotyczących informacji, które nie są szczególnie chronione w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych) jest dopuszczalne, po spełnieniu jednego z następujących warunków: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych (pkt 1), jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (pkt 2), jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (pkt 3), jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (pkt 4), 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 (pkt 5).

dostępie do informacji publicznej, informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej lub centralnym repozytorium, jest udostępniana na wniosek. Zatem przetwarzanie danych osób (wnioskodawców) o dostęp do informacji publicznej odbywa się na podstawie przepisów właśnie ustawy o dostępie do informacji publicznej, tj. na podstawie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. W takiej sytuacji pozyskiwanie zgody wnioskodawcy jest nie tylko zbędne i wprowadza w błąd osobę, która udostępnia swoje dane osobowe, ale przede wszystkim bezpodstawne ze względu na zasady wynikające z przepisów ustawy o dostępie do informacji publicznej.

Jak stanowi art. 14 ust. 1 ustawy o dostępie do informacji publicznej, udostępnianie informacji publicznej na wniosek następuje w sposób i w formie zgodny z wnioskiem, chyba że środki techniczne, którymi dysponuje podmiot obowiązany do udostępnienia, nie umożliwiają udostępnienia informacji w sposób i w formie określonych we wniosku. Zatem dla realizacji prawa dostępu do informacji publicznej nie zawsze jest potrzebne pozyskiwanie przez podmiot udostępniający informację publiczną danych osobowych, w zakresie wskazanym w formularzu wniosku. Bowiem to wnioskodawca decyduje w jakiej formie oczekuje zrealizowania prawa dostępu do informacji publicznej – korzystając z praw przysługujących mu na podstawie przepisów ustawy o dostępie do informacji publicznej - wskazując w tym celu, np. adres do korespondencji, albo adres poczty elektronicznej i takie dane osobowe zobowiązany jest jedynie podać.

Odwołując się do orzecznictwa sądowego, GIODO wskazał na wyrok Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 10 maja 2012 r. (sygn. IISAB/Łd 46/12), w którym sąd orzekł, iż za wniosek o udzielenie informacji publicznej uznać można przesłanie zapytania drogą elektroniczną, i to nawet, gdy do jej autoryzacji nie zostanie użyty podpis elektroniczny. Postępowanie w sprawie udzielenia informacji publicznej ma uproszczony i odformalizowany charakter, a osoba zadająca pytanie nie musi być nawet w pełni zidentyfikowana, nie musi bowiem wykazywać interesu prawnego, ani interesu faktycznego. Przepisy K.p.a. mogą być stosowane tylko w przypadkach określonych w ustawie o dostępie do informacji publicznej. Ta natomiast nie daje możliwości zastosowania art. 64 § 2 K.p.a., tj. pozostawienia wniosku bez rozpoznania. Podobne stanowisko zajął Wojewódzki Sąd Administracyjny w Gliwicach w wyroku z dnia 24 lutego 2012 r. (sygn. IV SAB/GI 75/11).

Należy zwrócić uwagę także na to, że przetwarzanie danych osobowych powinno odbywać się zgodnie z zasadami legalizmu, adekwatności oraz związania celem,

wynikającymi z art. 26 ust. 1 pkt 1-3 ustawy o ochronie danych osobowych[391]. Podkreślenia wymaga, że nawet jeśli administrator danych pozyskuje dane, co do przetwarzania których nie jest wymaga zgoda osoby, której dane dotyczą, bo zastosowanie znajdzie inna przesłanka z art. 23 ustawy, to każdy administrator danych zobowiązany jest do realizacji wszystkich innych obowiązków, które nakładają na niego przepisy ustawy o ochronie danych osobowych, np. do wykonania obowiązku informacyjnego z art. 24 lub 25 ustawy.

W udzielonej odpowiedzi poinformowano, że na stronach Biuletynu Informacji Publicznej (BIP) dostępny jest nowy formularz wniosku o udostępnienie informacji publicznej spełniający wymogi ustawy o ochronie danych osobowych. Ponieważ jednak informacja ta nie znalazła potwierdzenia na stronach BIP, GIODO prowadzi w tej sprawie dalszą korespondencję.

Wystąpienie GIODO z dnia 13 grudnia 2013 r.[392] do jednej z uczelni wyższej dotyczyło podjęcia stosownych działań w celu wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych osób, które odwiedzają studenta w akademiku.

W związku z pozyskaniem informacji, iż dowody osobiste osób odwiedzających studenta w akademiku jednej z wyższych uczelni były przechowywane, na czas tych odwiedzin, w portierni domu studenckiego, GIODO zwrócił się o wyeliminowanie tej praktyki jako zbędnej dla realizacji zakwaterowania studenta w akademiku i weryfikowania tożsamości osób go odwiedzających, jak również o uwzględnienie w swojej działalności zasad ochrony danych osobowych, wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

Organ do spraw ochrony danych osobowych zwrócił uwagę, że w procesie każdego przetwarzania danych osobowych, ustawa obliguje podmioty przetwarzające dane osobowe do przestrzegania zasad wyrażonych w jej przepisach na każdym etapie przetwarzania tych danych, w tym na etapie ich pozyskiwania, utrwalania, przechowywania i udostępniania. Administrator danych osobowych może przetwarzać dane osobowe, o ile istnieje ku temu podstawa prawa legalizująca takie działanie. Podstawa ta winna znajdować odzwierciedlenie

[391] Przepisy te stanowią, iż obowiązkiem administratora danych osobowych jest zapewnienie, aby dane były: 1) przetwarzane zgodnie z prawem, 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2, 3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
[392] DOLiS-035-3568/13

w brzmieniu obowiązujących, w zakresie ochrony danych osobowych, aktów prawnych o charakterze powszechnie obowiązującym, takich jak ustawa. Obowiązkiem administratora danych jest dokonanie rzetelnej analizy na etapie poprzedzającym dokonywanie każdej operacji na danych osobowych, dla jakich celów następuje pozyskiwanie, przechowywanie czy udostępnianie określonego rodzaju danych. Cel zbierania danych powinien być oznaczony i zgodny z prawem, a dalsze przetwarzanie danych niezgodne z tym celem jest niedopuszczalne. Cel przetwarzania danych osobowych nie jest jednak wynikiem arbitralnej decyzji administratora danych, oderwanym od okoliczności przetwarzania. Ustalając cel, zawsze indywidualnie należy go ocenić i odwołać się do kontekstu przetwarzania. Cel przetwarzania danych powinien zostać zakomunikowany przed ich pozyskaniem tj. zainteresowany powinien znać cel przetwarzania jego danych najpóźniej w momencie, w którym zbierane są jego dane osobowe. W szczególności zatem, zakres każdorazowo żądanych danych osobowych powinien być merytorycznie poprawny i adekwatny 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 swymi 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[393]. Równocześnie organ do spraw ochrony danych wskazał, że administrator danych ma obowiązek zapewnienia bezpiecznego przebiegu procesu przetwarzania danych osobowych, w sposób odpowiadający przepisom rozdziału 5 ustawy, jak również przepisom rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Rzetelne przestrzeganie powyższych zasad stanowi m. in. gwarancje właściwego poszanowania praw osób, których dane dotyczą. Przetwarzanie danych z dowodu osobistego nie będzie zatem niezgodne z prawem, jeśli będzie znajdowało stosowną podstawę prawną i nie będzie prowadziło do gromadzenia danych w zakresie szerszym niż jest to konieczne dla realizacji celu ich przetwarzania. Jednocześnie, co istotne,

[393] zob. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r. sygn. akt II SA/Wa 917/2005.

przetwarzanie danych nie może odbywać się w sposób, który narusza obowiązujące przepisy prawa.

Mając na uwadze powyższe stwierdzić wypada, iż o ile sam sposób pozyskiwania danych osobowych jest z punktu widzenia ustawy o ochronie danych osobowych obojętny[394], to czynność przetrzymywania dokumentu tożsamości budziła już uzasadnione zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych. Należy zwrócić uwagę na fakt, iż takie działanie budzi istotne zastrzeżenia nie tylko z punktu widzenia wymogu przetwarzania danych w zakresie adekwatnym do celu ich przetwarzania, bowiem nie może dochodzić do pozyskiwania szerszego zakresu, niż jest to konieczne dla realizacji celu, w jakim dane są przetwarzane. Zgodnie z art. 33 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. zm.) dowodu osobistego nie wolno zatrzymywać, z wyjątkiem przypadków określonych w ustawie. Zatrzymanie cudzego dowodu osobistego stanowi wykroczenie stypizowane w art. 55 ust. 1 pkt 2 cytowanej ustawy. Przepis ten stanowi, że kto zatrzymuje bez podstawy prawnej cudzy dowód osobisty podlega karze ograniczenia wolności albo karze grzywny. Orzekanie w sprawach, o których mowa w art. 55 ust. 1, następuje 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.).

Powszechnie obowiązujące przepisy prawa, w tym ustawy o ewidencji ludności i dowodach osobistych, mają charakter nadrzędny nad regulaminami i innymi przepisami wewnętrznymi uczelni. Treść wewnętrznych przepisów uczelni nie wpływa na wyłączenie mocy obowiązującej ustawy, która stanowi źródło powszechnie obowiązującego prawa Rzeczypospolitej Polskiej, stosownie do brzmienia art. 87 ust. 1 Konstytucji Rzeczypospolitej Polskiej. Nie może zatem dochodzić do formułowania przepisów wewnętrznych uczelni w sprzeczności z przepisami powszechnie obowiązującego prawa. Wprawdzie sposób pozyskiwania danych zawartych w dowodzie osobistym to kwestia drugorzędna w stosunku do spełnienia, opisanych wyżej, warunków legalnego przetwarzania danych osobowych, jak i przetwarzania ich w zakresie niezbędnym dla celu tego przetwarzania, niemniej jednak zatrzymanie cudzego dowodu osobistego - jako sposób pozyskiwania i dalszego przetwarzania danych osobowych wyszczególnionych w dowodzie tożsamości - nie może

[394] por. wyrok Naczelnego Sądu Administracyjnego z dnia 19 grudnia 2001 r. sygn. akt II SA 2869/00, czy też wyrok NSA z dnia 7 listopada 2003 r. sygn. akt II SA 1432/02.

pozostawać w sprzeczności z zasadami wynikającymi z przepisów ustawy o ochronie danych osobowych i przepisami szczególnymi, w szczególności ustawą o ewidencji ludności i dowodach osobistych. Co więcej, pozyskiwanie danych osobowych zawartych w dowodzie osobistym nie powinno być utożsamiane z zatrzymywaniem dowodu osobistego dla realizacji celu weryfikacji tożsamości osoby odwiedzającej studenta w akademiku.

W świetle przepisów dotyczących ochrony danych osobowych i przepisów szczególnych, w tym ustawy o ewidencji ludności i dowodach osobistych, niedopuszczalne jest uznanie zatrzymania cudzego dowodu osobistego jako legalnego sposobu pozyskiwania i dalszego przetwarzania danych osobowych, wyszczególnionych w dowodzie tożsamości, dotyczących osób odwiedzających studenta w akademiku. Takie działanie budzi zastrzeżenia pod kątem legalności, zasadności i celowości (art. 23 ustawy i art. 26 ust. 1 pkt 1-4 ustawy) działania uczelni wyższej i w związku z tym konieczne jest wyeliminowanie nieprawidłowych praktyk polegających na zatrzymywaniu, na portierni domu studenckiego, dowodów osobistych należących do osób odwiedzających studenta w akademiku.

W odpowiedzi pismem z dnia 14 stycznia 2014 r. poinformowano, że problem ten został rozwiązany poprzez zmianę przepisów wewnętrznych uczelni.

W wystąpieniu z dnia 20 grudnia 2013 r.[395] Generalny Inspektor Ochrony Danych Osobowych wskazywał Komendantowi Głównemu Policji potrzebę podjęcia działań mających na celu zaznajomienie funkcjonariuszy Policji z podstawowymi zagadnieniami dotyczącymi ochrony danych osobowych, w szczególności kwestii związanych z pozyskiwaniem danych osobowych oraz przepisów karnych ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych, w tym uwrażliwienie funkcjonariuszy Policji na fakt, że do Generalnego Inspektora Ochrony Danych Osobowych nie należy kierować wniosków o udostępnienie danych osobowych, gdyż stosownie do art. 12 ww. ustawy ich udostępnianie pozostaje poza zakresem kompetencji organu.

Impulsem do skierowania wystąpienia przez Generalnego Inspektora Ochrony Danych Osobowych były m.in. zapytania kierowane do niego w kwestiach dotyczących przetwarzania danych osobowych w sprawach prowadzonych przez funkcjonariuszy Policji. Funkcjonariuszom największe problemy sprawiają m. in. kwestie związane z kwalifikacją prawną prowadzonych spraw, kwestie odnoszące się do definicji ustawowych określonych

[395] DOLiS-035-4126-13

w art. 7 ustawy o ochronie danych osobowych, a także prawidłowe adresowanie wniosków o udostępnienie danych ze zbioru danych osobowych, które błędnie kierowane są do Generalnego Inspektora Ochrony Danych Osobowych. W dodatku do Generalnego Inspektora wpłynął wniosek o udostępnienie danych ze zbioru danych osobowych opierający się na nieaktualnej podstawie prawnej (tj. na uchylonym art. 29 ustęp 1 ustawy o ochronie danych osobowych). Wypada stwierdzić, że kierowanie pism opierających się na uchylonych przepisach nie przystoi funkcjonariuszom publicznym, którzy mają dbać o kulturę prawną obywateli.

Generalny Inspektor Ochrony Danych Osobowych podkreślił, że nie jest organem właściwym do orzekania, czy dane działanie bądź zaniechanie wypełniło znamiona któregoś z czynów zabronionych określonych w ustawie o ochronie danych osobowych. Zadania Generalnego Inspektora zostały określone w art. 12 ustawy o ochronie danych osobowych[396]. W szczególności wypada podkreślić, że zgodnie z przewidzianymi w ustawie kompetencjami (art. 12 pkt 4) Generalny Inspektor prowadzi rejestr zbiorów danych, a nie rejestr wszelkich danych osobowych. Stąd też stosownie do treści przepisów szczególnych dane z określonych zbiorów udostępniają, określone w tychże przepisach, właściwe przedmiotowo organy. Dlatego też Generalny Inspektor nie może rozpatrywać takich wniosków, ani tym bardziej udostępniać danych, których nie posiada. Przepis art. 15 § 2 kodeksu postępowania karnego stanowi, iż wszystkie instytucje państwowe i samorządowe są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne w terminie wyznaczonym przez te organy. Ze sformułowania tego przepisu wynika w sposób oczywisty, że obowiązek ten dotyczy wyłącznie udzielenia pomocy w zakresie prowadzonego postępowania karnego. Organy ścigania mają prawo do pomocy instytucji państwowych i samorządowych, jeżeli dokonują czynności w ramach art. 307 i 308 oraz w toku wszczętego postępowania przygotowawczego. Żądanie pomocy nie może przekraczać zakresu działania

[396] Do zadań Generalnego Inspektora Ochrony Danych Osobowych należą: 1) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych, 2) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych, 3) zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji, o których mowa w pkt 2, 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.), 4) prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach, 5) opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych, 6) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych, 7) uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

danych instytucji. Udzielenie pomocy w rozumieniu § 2 nie obejmuje obowiązku współdziałania w ramach tzw. czynności operacyjno-rozpoznawczych[397].

Ponadto mając na uwadze wskazany wyżej problem wskazać należało, że Generalny Inspektor Ochrony Danych Osobowych nie może ingerować w sprawy zastrzeżone do kompetencji innych organów (w tym organów ścigania i wymiaru sprawiedliwości), co potwierdził Naczelny Sąd Administracyjny w wyroku z dnia 2 marca 2001 r. stwierdzając, że *„(...) Generalny Inspektor (...) nie jest organem kontrolującym ani nadzorującym nieprawidłowość 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*"[398]. Podobne stanowisko zostało wyrażone także w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 27 lutego 2012 r.: „*Generalny Inspektor Ochrony Danych Osobowych nie jest władny do kontrolowania podejmowanych przez organ czynności procesowych w postępowaniu z wykorzystaniem danych osobowych, czy to sądowym, czy to prokuratorskim, bądź prowadzonym przez Policję na zlecenie Prokuratury"*[399].

Mając na uwadze powyższe, Generalny Inspektor zwrócił się o podjęcie stosownych działań mających na celu uwrażliwienie funkcjonariuszy Policji na podstawowe zagadnienia związane z ochroną danych osobowych, jak również poinformowanie Generalnego Inspektora Ochrony Danych Osobowych o podjętych w przedmiotowej sprawie działaniach, stosownie do treści art. 19a ustęp 3 ustawy o ochronie danych osobowych.

W odpowiedzi Komendant Główny Policji poinformował o działaniach wykonanych celem realizacji zadań wskazanych w wystąpieniu, m.in. o zaznajomieniu funkcjonariuszy Policji z podstawowymi zagadnieniami dotyczącymi ochrony danych osobowych.

8.2. Działalność informacyjna

Do działalności informacyjnej GIODO, podobnie jak w latach ubiegłych, wykorzystywane były różnorodne kanały komunikacyjne, takie jak:

- strona internetowa (na bieżąco aktualizowana i uzupełniana),

[397] Kodeks postępowania karnego. Tom I. Komentarz do art. 1-424, Jan Gajewski, Sławomir Steinborn, LEX 2013.
[398] sygn. akt II SA 401/00
[399] sygn. akt II SA/Wa 2848/11

- Infolinia (czynna w godzinach pracy Biura),
- Newsletter (zawierający najnowsze informacje o działalności GIODO),
- konferencje i seminaria naukowe (organizowane przez GIODO, a także inne instytucje z udziałem GIODO lub pracowników Biura),
- szkolenia prowadzone przez ekspertów Biura,
- kampanie edukacyjne i informacyjne realizowane we współpracy z innymi instytucjami, w tym również z mediami,
- indywidualne spotkania z interesantami podczas dyżurów pełnionych przez Zastępcę GIODO i pracowników departamentów,
- publikacje książkowe powstające przy udziale GIODO i pracowników Biura,
- media tradycyjne i elektroniczne.

8.2.1. Współpraca ze środkami masowego przekazu

1. Stałe kontakty z mediami

Wzorem lat ubiegłych, w 2013 r. organ do spraw ochrony danych osobowych kontynuował stałą współpracę z mediami, polegającą na przekazywaniu do publikacji materiałów informacyjno-edukacyjnych, w tym wydanych decyzji, wystąpień, sygnalizacji, pism GIODO, jak i gotowych do druku opracowań konkretnych zagadnień z zakresu ochrony danych osobowych. Współpraca prowadzona była 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 (jak np. Dziennik Internautów czy lex.pl), w tym będącymi odpowiednikami prasy drukowanej. Upowszechnianiu wiedzy z zakresu ochrony danych osobowych służyła też publikacja wyjaśnień GIODO w czasopismach kobiecych, takich jak np. „Twoje Imperium" czy „Świat Kobiety". W 2013 r. stała współpraca GIODO ze stacjami telewizyjnymi i radiowymi, m.in. z Informacyjną Agencją Radiową, Polskim Radiem Jedynką, Polskim Radiem 24, Radiem TOK FM, Radiem dla Ciebie, TVP INFO, Telewizją Polsat, Superstacją czy TVN24, zaowocowała wieloma programami o tematyce ochrony danych osobowych. Również współpracujące z GIODO agencje informacyjne - PAP, KAI

i Newserią - poświęcały wiele uwagi tej problematyce. Dodatkowo Newseria uruchomiła, w maju 2013 r., specjalny kanał informacyjny Generalnego Inspektora Ochrony Danych Osobowych.

W 2013 r. w prasie, radiu, telewizji i Internecie opublikowanych lub wyemitowanych zostało ponad **170** materiałów prasowych o tematyce ochrony danych. Duża część z nich jest dostępna na stronie internetowej GIODO (www.giodo.gov.pl).

2. Odpowiedzi na indywidualne pytania dziennikarzy

Stałą formą kontaktów GIODO z dziennikarzami było udzielanie im odpowiedzi na pytania, które dotyczyły nie tylko ochrony danych osobowych, ale także innych, związanych z tą dziedziną, kwestii prawnych.

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

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii, zwłaszcza modelu *cloud computing*,
- funkcjonowanie portali społecznościowych w kontekście wykorzystywania 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, ze szczególnym uwzględnieniem telemarketingu,
- ochrona danych osobowych w procesie rekrutacji i zatrudnienia,
- zabezpieczanie danych osobowych jako główny problem w związku ze stosowaniem nowych technologii,
- upublicznianie przez jednostki samorządu terytorialnego w BIP uchwał, decyzji czy protokołów z danymi osobowymi osób fizycznych,
- przetwarzanie danych osobowych dłużników,
- możliwość stosowania monitoringu wizyjnego przez podmioty inne niż ustawowo upoważnione,
- pozyskiwanie danych osobowych przez organizatorów konkursów internetowych i SMS'owych,

- kompetencje GIODO w stosunku do kościołów i związków wyznaniowych w kontekście problemu apostazji, czyli występowania z kościoła lub związku,
- przetwarzanie danych osobowych przez spółdzielnie i wspólnoty mieszkaniowe,
- wycieki danych od operatorów telekomunikacyjnych.

W 2013 r. GIODO udzielił – pisemnie lub telefonicznie – ponad **320** odpowiedzi.

3. Wywiady i wystąpienia

Tematyka wywiadów radiowych i telewizyjnych oraz udzielonych w 2013 r. dziennikarzom prasy drukowanej i internetowej, dotyczyła zarówno zasad ochrony danych osobowych określonych w ustawie o ochronie danych osobowych, jak i w przepisach branżowych.

Oprócz opisanych wcześniej tematów zainteresowanie mediów budziło także przetwarzanie danych osobowych na potrzeby zatrudnienia, prowadzenia marketingu, mieszkalnictwa, oświaty i służby zdrowia, a także ochrony danych osobowych w kontekście rozwoju nowoczesnych technologii. Dziennikarzy interesowało również, jak bezpiecznie korzystać z urządzeń mobilnych, portali internetowych, zwłaszcza społecznościowych, m.in. takich jak Facebook. Wśród innej poruszanej w rozmowach problematyki związanej z wykorzystaniem nowoczesnych technologii, wymienić można: Internet przedmiotów, monitorowanie pracowników, instalowanie monitoringu wizyjnego czy inteligentnych liczników energetycznych. Również tworzenie systemu informacji w ochronie zdrowia było tematem częstych wystąpień medialnych GIODO w 2013 r.

Kolejnymi komentowanymi i wyjaśnianymi przez GIODO zagadnieniami były: pozyskiwanie przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA) danych osobowych obywateli, w tym Polaków, pozyskiwanie danych tzw. hejterów, czyli osób zamieszczających w sieci obraźliwe wpisy, kompetencje GIODO w stosunku do apostatów oraz nowe podejście do rozpatrywania spraw w tym zakresie w związku z wyrokami WSA i NSA. Ponadto GIODO niejednokrotnie udzielał wywiadów poświęconych wyciekom danych osobowych, wyłudzaniu bądź wykradaniu danych osobowych, bezpiecznemu korzystaniu z Internetu oraz zbliżeniowych kart płatniczych, pozostawianiu dowodu

osobistego w zastaw za wypożyczany sprzęt i zagrożeniom z tym związanym, a także dopuszczalności tworzenia przez przedsiębiorców profili osobowych klientów.

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.

W 2013 r. GIODO udzielił blisko **290** wywiadów.

4. Konferencje prasowe

W związku z potrzebą nagłośnienia niektórych wydarzeń lub upublicznienia stanowiska GIODO w istotnych dla ochrony danych osobowych sprawach, GIODO w 2013 roku zorganizował **10 konferencji prasowych**, które poświęcone były:

- bezpieczeństwu danych osobowych przetwarzanych przy wykorzystaniu systemu Elektronicznej Weryfikacji Uprawnień Świadczeniobiorców (eWUŚ) oraz planowanemu uruchomieniu Zintegrowanego Informatora Pacjenta (9.01.2013 r.),
- obchodom VI Dnia Ochrony Danych Osobowych w Polsce i w Brukseli (28.01.2013 r. w Warszawie oraz 22.01.2013 r. w Brukseli),
- omówieniu wątpliwości prawnych związanych z wejściem w życie z dniem 1 stycznia 2013 r. amerykańskiej ustawy o ujawnianiu informacji finansowych o rachunkach zagranicznych na cele podatkowe (FATCA), która zobowiązuje zagraniczne instytucje finansowe, w tym banki, do identyfikacji swoich klientów będących obywatelami USA i przekazywania ich danych do urzędu podatkowego Stanów Zjednoczonych (13.02.2013 r.),
- bezpieczeństwu zbliżeniowych kart płatniczych i zastrzeżeniom GIODO dotyczącym stosowanej w nich, niewystarczająco dopracowanej technologii NFC, która zagraża bezpieczeństwu zarówno danych osobowych, jak i operacjom finansowym (29.03.2013 r.),
- podstawowym zasadom ochrony danych osobowych, a także zagrożeniom, jakie dla ochrony danych i prywatności stanowi rozwój nowych technologii. Omówione zostały zasady wykorzystywania danych osobowych przez urzędy administracji publicznej, m.in. na potrzeby realizacji przez gminy tzw. ustawy śmieciowej. Konferencja prasowa odbyła się w związku z III Dniem Otwartym GIODO (Poznań, 6.05.2013 r.),

- pozyskiwaniu przez gminy zbyt szerokiego zakresu danych osobowych na potrzeby realizacji zadań dotyczących gospodarki odpadami. Wskazano, do pozyskiwania jakich danych gminy są uprawnione na mocy przepisów ustawy o utrzymaniu czystości i porządku w gminach. Przypomniano też podstawowe zasady, jakich gminy muszą przestrzegać pozyskując dane osobowe, ze szczególnym uwzględnieniem zasad legalizmu, adekwatności oraz celowości, o których mowa w ustawie o ochronie danych osobowych. Ponadto przedstawione zostały przykłady niezgodnego z prawem żądania gmin i poinformowano o działaniach, jakie organ ds. ochrony danych osobowych będzie podejmował zgodnie ze swoimi kompetencjami (27.05.2013 r.),
- programowi edukacyjnemu GIODO „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Omówione zostały innowacyjne sposoby przekazywania wiedzy wypracowane przez szkoły biorące udział w 3. edycji programu, a także problemy związane z przetwarzaniem danych osobowych w sektorze oświaty (3.06.2013 r.),
- 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, zorganizowanej przez GIODO w dniach 23-26.09.2013 r. w Warszawie. Podczas pierwszej konferencji prasowej poinformowano o wydarzeniu i przedstawiono główne tematy obrad (13.09.2013 r.). Druga - odbyła się w przerwie obrad i zaprezentowano na niej główne ustalenia i przyjęte dokumenty (25.09.2013 r.).

Ponadto w 2013 r. GIODO – jako ekspert i gość honorowy – uczestniczył w konferencjach prasowych zorganizowanych przez współpracujące z Biurem instytucje. Dotyczyły one:

- wdrażania inteligentnego opomiarowania, a zwłaszcza instalowania inteligentnych liczników energetycznych. Odbyła się ona w przerwie debaty pt. Prywatność i dane osobowe w inteligentnych sieciach energetycznych", w której udział – poza GIODO – wzięli m.in. prezes Urzędu Regulacji Energetyki, prawnicy a także przedstawiciele firm dystrybuujących energię elektryczną. Podczas spotkania z mediami GIODO podkreślił, że dane pomiarowe są danymi osobowymi, do przetwarzania których muszą być spełnione określone warunki. Organizatorem wydarzenia było Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej (26.06.2013 r.),

- funkcjonowania Zintegrowanego Informatora Pacjenta (ZIP), czyli ogólnopolskiego serwisu, za pomocą którego zarejestrowani użytkownicy mają wgląd w dane o udzielonych im świadczenia zdrowotnych finansowanych ze środków publicznych. GIODO odniósł się do tego projektu w kontekście ochrony danych osobowych i prywatności, podczas konferencji prasowej, której organizatorem był Narodowy Fundusz Zdrowia (9.07.2013 r.),
- zjawiska kradzieży tożsamości, podczas której zaprezentowano wyniki badań dotyczących świadomości i zachowań związanych z zabezpieczaniem danych osobowych przez osoby fizyczne, a także przedstawiono dane statystyczne dotyczące prób wyłudzenia kredytów z wykorzystaniem skradzionej tożsamości. Organizatorem konferencji była firma Fellowes – od 2005 r. realizująca kampanię edukacyjną „Nie daj się okraść, chroń swoją tożsamość" (23.10.2013 r.).

5. Akcje informacyjno-promocyjne

a) Dzień Ochrony Danych Osobowych

Do stałych akcji informacyjno-promocyjnych należy organizacja Dnia Ochrony Danych Osobowych, która w 2013 r. została przeprowadzona po raz siódmy. W ramach Dni, podobnie jak w latach ubiegłych, w Brukseli odbyło się spotkanie GIODO z eurodeputowanymi (22 stycznia 2013 r.). Głównymi tematami spotkania były kwestia reformy ochrony prywatności, a także europejska strategia wobec cloud computingu i projekt INDECT. Tradycyjnie też miał miejsce uroczysty wieczór w siedzibie Stałego Przedstawicielstwa Rzeczypospolitej Polskiej przy Unii Europejskiej (22 stycznia 2012 r.), zorganizowany we współpracy z polskim ambasadorem przy Unii Europejskiej. Uczestniczyli w nim polscy posłowie do Parlamentu Europejskiego, rzecznicy ochrony danych osobowych z państw UE z Peterem Hustinxem, Europejskim Rzecznikiem Ochrony Danych Osobowych na czele, przedstawiciele Komisji Europejskiej oraz innych polskich i unijnych instytucji mających siedzibę w Brukseli. W dniach 23-25 stycznia 2013 r. odbyła się międzynarodowa konferencja „Komputery, ochrona danych i prywatności", podczas której jeden z paneli poświęcony był ochronie prywatności w Polsce, a jego gospodarzem był Generalny Inspektor Ochrony Danych Osobowych. Ze względu na fakt, że w 2013 r. minęło 15 lat od czasu ustanowienia konstytucyjnych i ustawowych ram ochrony danych osobowych w Polsce, panel pt. „Od *Solidarności* do społeczeństwa nadzorowanego. Dylematy ochrony prywatności w Polsce"

poświęcono analizie wykorzystywania danych osobowych przez podmioty publiczne, skupiając się m.in. ma kwestiach nadzoru, retencji danych i prawach podmiotu danych. Natomiast w Polsce, obchody Dnia Ochrony Danych Osobowych przebiegały pod hasłem „Dane osobowe w służbie zdrowia i w badaniach klinicznych" i odbyły się 28 stycznia. Tego dnia tradycyjnie zorganizowano Dzień Otwarty, na który złożyły się:

- konferencja „Dane osobowe w służbie zdrowia i w badaniach klinicznych" z udziałem przedstawicieli Rzecznika Praw Pacjenta, Ministerstwa Administracji i Cyfryzacji, Centrum Systemów Informacyjnych Ochrony Zdrowia, Wojskowej Akademii Technicznej, a także reprezentantów środowiska naukowego oraz jednostek ochrony zdrowia i firm oraz instytucji działających na rzecz tego sektora,
- bezpłatne porady i konsultacje ekspertów z Biura GIODO,
- panel dyskusyjny „Ochrona danych w służbie zdrowia i w badaniach klinicznych" zorganizowany przez GIODO oraz redakcję „Dziennika Gazety Prawnej" (8 stycznia 2013 r. w siedzibie Redakcji), a publikacja jego zapisu miała miejsce 28 stycznia 2013 r.

Informacje o wszystkich wymienionych wyżej wydarzeniach dotyczących Dnia Ochrony Danych Osobowych zaowocowały publikacją licznych artykułów prasowych i internetowych związanych z jego tematem przewodnim.

b) Debaty

Nagłośnianiu istotnych, z punktu widzenia ochrony danych osobowych, zagadnień służą również organizowane w mediach debaty. W roku sprawozdawczym GIODO był współorganizatorem debaty w Redakcji „Dziennika Gazety Prawnej", która odbyła się 19 lipca 2013 r. W debacie tej, pt. „Inteligentne liczniki – korzyści i zagrożenia", uczestniczyli przedstawiciele Urzędu Regulacji Energetyki, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, RWE Stoen Operator Sp. z o.o., Federacji Konsumentów oraz zespołu prawa telekomunikacyjnego i ochrony danych osobowych w Kancelarii Wierzbowski Eversheds.

c) Wakacyjna kampania informacyjna

W 2013 r. GIODO po raz kolejny włączył się do akcji wakacyjnej organizowanej przez Urząd Ochrony Konkurencji i Konsumentów pod hasłem „Przed wakacjami - co warto wiedzieć?". Na jej potrzeby przygotowany został wideoporadnik poświęcony temu, jak należy dbać o ochronę danych w czasie wakacji. GIODO udzielał dzieciom i młodzieży krótkich, praktycznych wskazówek na temat tego, np. czy wypożyczalnia może żądać, abyśmy w zastaw za wypożyczony sprzęt zostawili dokument potwierdzający tożsamość (np. dowód osobisty czy legitymację szkolną), jakich danych można od nas żądać w hotelu czy ośrodku wypoczynkowym, skoro zniesiono obowiązek meldunkowy przy pobytach poniżej 3 miesięcy, czy na portalu społecznościowym powinniśmy podawać informacje, kiedy i dokąd wyjeżdżamy. Ponadto GIODO wyjaśniał, czy korzystanie z sieci wi-fi oraz płatności kartą zbliżeniową lub telefonem jest bezpieczne, jakie zabezpieczenia komputera, telefonu czy smartfonu zastosować, by w sytuacji zgubienia czy kradzieży tych urządzeń nikt obcy nie miał dostępu do zapisanych w nich danych. Poradnik został zamieszczony na stronie internetowej GIODO, a linki do niego znalazły się na stronach internetowych 30 innych urzędów i instytucji biorących udział w tej akcji.

Tematy poruszane w poradniku GIODO zostały podjęte przez większość mediów zarówno tradycyjnych, jak i elektronicznych.

6. Infolinia

Ważną rolę w działalności informacyjnej GIODO pełniła, działająca w godzinach pracy Biura, Infolinia - telefon informacyjny. W 2013 r. za jej pośrednictwem udzielono wyjaśnień około **12 tysiącom** osób. Utworzenie infolinii było odpowiedzią na ogromne zainteresowanie zagadnieniami dotyczącymi ochrony danych osobowych zarówno osób, których dane dotyczą, jak i osób, firm i instytucji, które przetwarzają (wykorzystują) dane osobowe.

7. Newsletter

W 2013 r. GIODO kontynuował wydawanie Newslettera, dostarczanego każdemu zainteresowanemu jego otrzymywaniem, poprzez zarejestrowanie się za pośrednictwem strony internetowej GIODO. W 2013 r. ukazało się **6** numerów tej elektronicznej formy biuletynu. Newsletter stanowi źródło najświeższych informacji o działalności Generalnego Inspektora Ochrony Danych Osobowych, m.in. o: wydanych decyzjach, wystąpieniach

i sygnalizacjach kierowanych do różnych podmiotów, najważniejszych zmianach w przepisach prawa, aktualnych opiniach i stanowiskach GIODO, planowanych konferencjach i seminariach, jak też opiniach Grupy Roboczej Art. 29, której członkiem jest Generalny Inspektor.

8.2.2. Dni Otwarte Generalnego Inspektora Ochrony Danych Osobowych

Dni Otwarte GIODO organizowane w różnych miejscach w Polsce to nowa inicjatywa Generalnego Inspektora Ochrony Danych Osobowych, podjęta w poprzednim roku sprawozdawczym. Jest ona 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.

W dniach 6-7 maja 2013 r. zorganizowany został w Poznaniu **III Dzień Otwarty GIODO,** w którym udział wzięło ponad 1000 osób. Generalny Inspektor Ochrony Danych Osobowych we współpracy z Prezydentem Miasta Poznania, Uniwersytetem Ekonomicznym w Poznaniu, Marszałkiem Województwa Wielkopolskiego, Wojewodą Wielkopolskim oraz Wielkopolską Izbą Przemysłowo-Handlową, przygotował szereg wydarzeń, w tym m.in. konferencję naukową poświęconą prawnym i ekonomicznym aspektom przetwarzania danych osobowych dla celów gospodarczych, a także cykl spotkań seminaryjno-szkoleniowych dla administracji publicznej.

Pierwszym wydarzeniem, które odbyło się w ramach III Dnia Otwartego GIODO, była konferencja szkoleniowa dla pracowników Urzędu Miasta Poznania oraz jednostek podległych i współpracujących z Urzędem. Poświęcona była aktualnym problemom stosowania przez organy samorządu terytorialnego, przepisów o ochronie danych osobowych w kontekście ich udostępniania i bezpieczeństwa oraz przepisów o dostępie do informacji publicznej. W czasie trwania konferencji czynne były stoiska informacyjne, przy których

eksperci (m.in. z Biura GIODO) udzielali bezpłatnych porad i informacji z zakresu ochrony danych osobowych oraz rozdawali materiały edukacyjno–informacyjne Biura GIODO.

W tym samym czasie, w siedzibie Wielkopolskiej Izby Przemysłowo - Handlowej w Poznaniu, z inicjatywy Prezesa Izby, odbył się Sejmik Gospodarczy nt. „Ochrona danych osobowych przez podmioty gospodarcze" z udziałem przedstawicieli rzemiosła i handlu.

W dniu 7 maja 2013 r. w Poznaniu odbyło się śniadanie GIODO z przedsiębiorcami**.** Pomysł organizowania spotkań z przedstawicielami biznesu w formule śniadania, zrodził się kilkanaście lat temu i jest wspólnym przedsięwzięciem firmy Iron Mountain i kolejnych Inspektorów. Dotąd śniadania odbywały się w Warszawie. III Dzień Otwarty GIODO stał się okazją, by tego typu wydarzenie po raz pierwszy zorganizować poza stolicą. Podczas śniadania GIODO z przedsiębiorcami, dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, przedstawił założenia reformy europejskich ram prawnych ochrony danych, najwięcej uwagi poświęcając wpływowi planowanych zmian na działalność sektora biznesu. Śniadanie było ponadto okazją do przedyskutowania z Generalnym Inspektorem Ochrony Danych Osobowych bieżących wątpliwości i problemów w relacjach pracodawca – pracownik, w szczególności w kwestii pozyskiwania przez pracodawców od związków zawodowych list osób objętych ochroną związkową.

Konferencja naukowa poświęcona prawnym i ekonomicznym aspektom przetwarzania danych osobowych dla celów gospodarczych była centralnym punktem III Dnia Otwartego GIODO. Gospodarzem tego wydarzenia był Uniwersytet Ekonomicznym w Poznaniu. Po jej oficjalnym otwarciu dr Wojciech Rafał Wiewiórowski, GIODO, wygłosił wykład pt. „Wspólny rynek przetwarzania danych osobowych w Unii Europejskiej", w którym podkreślił konieczność modernizacji unijnych przepisów prawa o ochronie danych osobowych w sposób, który najlepiej będzie odpowiadał konkurencyjnym wyzwaniom współczesnej globalnej gospodarki, przy zachowaniu wzmocnionej pozycji praw obywateli. Konferencję naukową poprzedziła uroczystość podpisania Porozumienia o współpracy pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a JM Rektorem Uniwersytetu Ekonomicznego w Poznaniu o współpracy w zakresie ochrony prywatności i danych osobowych.

Kolejnym wydarzeniem, które odbyło się w ramach III Dnia Otwartego GIODO w Poznaniu, była Konferencja szkoleniowa nt. aspektów ochrony danych osobowych w urzędach marszałkowskich**,** zorganizowana wspólnie z Marszałkiem Województwa

Wielkopolskiego. Konferencja koncentrowała się wokół tematów związanych z aktualnymi problemami stosowania zasad ochrony danych osobowych przez organy administracji publicznej, takich jak udostępnianie danych osobowych, dostęp do informacji publicznej czy bezpieczeństwo danych osobowych. Wzięli w niej udział przedstawiciele wszystkich urzędów marszałkowskich w Polsce odpowiedzialni za ochronę danych osobowych oraz przedstawiciele jednostek nadzorowanych przez marszałka województwa wielopolskiego.

Ostatnim punktem Dnia było szkolenie seminaryjne w Urzędzie Wojewódzkim w Poznaniu z udziałem kierownictwa i pracowników tego Urzędu nt. „Ochrony danych osobowych w działalności organów administracji państwowej".

8.2.3. Publikacje

„Ochrona danych osobowych w praktyce". Warszawa 2013, Wyd. PKN. Publikacja powstała na podstawie umowy o współpracy pomiędzy Polskim Komitetem Normalizacyjnym a Generalnym Inspektorem Ochrony Danych Osobowych. ISBN 978-83-275-1322-9.

W 2013 r. ukazał się podręcznik „Ochrona danych osobowych w praktyce", wydany przez Polski Komitet Normalizacyjny (PKN). Podczas prac nad publikacją autorzy z Polskiego Komitetu Normalizacyjnego współpracowali z Generalnym Inspektorem Ochrony Danych Osobowych i pracownikami Biura GIODO. Podręcznik zawiera całościowe opracowanie organizacji systemu bezpieczeństwa informacji w szeroko rozumianych procesach przemysłowych, zgodnie z uregulowaniami prawnymi i najlepszymi praktykami. Dostarcza wskazówek, jak zbudować sprawny System Zarządzania Bezpieczeństwem Informacji (SZBI), weryfikować go i udoskonalać, a także przeprowadzać analizę ryzyka, wykorzystując najnowsze technologie teleinformatyczne, jak RFID, NFC (Near Field Communication), identyfikację i weryfikację biometryczną, usługi geolokalizacyjne i inne. Uwzględnienie tych metod oraz dobrych praktyk pozwoli na wkomponowanie elementów zapewniających bezpieczeństwo zasobów informacyjnych zawierających dane osobowe już na etapie projektowania systemu, zgodnie z koncepcją *privacy by design*. Zapewnienie tego bezpieczeństwa wymaga bowiem odpowiednich działań na każdym etapie przetwarzania informacji, począwszy od procesu pozyskiwania i utrwalania, poprzez przechowywanie, wymianę, przekazywanie, a skończywszy na procesie jej kontrolowanego usuwania.

8.2.4. Szkolenia

1) Szkolenia podmiotów zewnętrznych

W ramach prowadzonej działalności edukacyjnej w 2013 roku, Generalny Inspektor Ochrony Danych Osobowych, podobnie jak w latach poprzednich, organizował nieodpłatne szkolenia z zakresu ochrony danych osobowych, skierowane do instytucji publicznych oraz innych podmiotów zainteresowanych podnoszeniem swoich kwalifikacji w tym obszarze.

Wśród podmiotów, które w 2013 r. zwróciły się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o przeprowadzenie szkolenia znalazły się: Agencja Rynku Rolnego, Agencja Rozwoju Mazowsza, Główny Inspektorat Weterynarii, Teatr Roma, Mazowiecka Jednostka Wdrażania Programów Unijnych, Naczelna Izba Lekarska, Inspektorat Wojskowej Służby Zdrowia, Krajowa Rada Spółdzielcza, Ośrodek Rozwoju Edukacji, Akademia Obrony Narodowej, Kancelaria Sejmu, Rządowe Centrum Legislacji, Sąd Okręgowy w Warszawie, Okręgowe Izby Radców Prawnych w Kielcach, Gdańsku, Krakowie i we Wrocławiu, Ministerstwa: Administracji i Cyfryzacji, Sprawiedliwości, Spraw Zagranicznych, Pracy i Polityki Społecznej, Finansów, Środowiska, a także Urzędy Marszałkowskie Województw: Dolnośląskiego, Wielkopolskiego, Lubuskiego, Małopolskiego Urzędu Wojewódzkiego w Krakowie i Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu oraz Urzędy Miast: Poznań, m.st. Warszawy.

Ponadto Generalny Inspektor Ochrony Danych Osobowych przeprowadził szkolenia dla trenerów użytkowników KSI w Komendzie Głównej Policji oraz dla przedstawicieli Komendy Wojewódzkiej Policji w Radomiu, Komendy Stołecznej Policji w Warszawie, Komendy Głównej Państwowej Straży Pożarnej, a także Mazowieckiego Oddziału Żandarmerii Wojskowej oraz jednostek jej podległych.

Niektóre szkolenia miały ogólnopolski zasięg, jak szkolenie pt. „ABC Ochrony Danych Osobowych", realizowane w ramach IV edycji ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", w którym udział wzięło ponad 150 osób – przedstawicieli 139 placówek zgłoszonych do IV edycji programu w roku szkolnym 2013/2014, szkolenie dla dyrektorów szkół, przedszkoli oraz przedstawicieli samorządu terytorialnego zorganizowane przez Kuratorium Oświaty w Warszawie Delegatura Radom, w którym uczestniczyło około 800 osób, czy ogólnopolskie szkolenie z zakresu ochrony

danych osobowych w izbach, cechach i firmach rzemieślniczych, którego gospodarzem była Wielkopolska Izba Rzemieślnicza w Poznaniu.

W sumie w 2013 r. przeprowadzono **60 szkoleń** podmiotów zewnętrznych, których wykaz znajduje się w załączniku nr 5. Podkreślenia wymaga, że wykaz ten obejmuje tylko szkolenia *sensu stricte,* ale można uzupełnić go także o niektóre spotkania, seminaria, warsztaty i konferencje o charakterze dydaktycznym czy popularnonaukowym, ponieważ przebiegały one w formule szkolenia. Przykładem może być udział zastępcy GIODO w szkoleniu dla kujawsko-pomorskich sekretarzy gmin i powiatów, które odbyło się 13 czerwca 2013 r. w Białych Błotach podczas Forum Sekretarzy Województwa Kujawsko-Pomorskiego, czy spotkanie GIODO z prezesami, dyrektorami, sędziami, pracownikami sadów oraz reprezentacją prokuratorów apelacji wrocławskiej, które z inicjatywy Sądu Apelacyjnego we Wrocławiu odbyło się 12 lutego 2013 r. Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych w wystąpieniu pt. „Ochrona danych osobowych w praktyce sądów", omówił podstawowe pojęcia i zasady związane z ochroną danych osobowych w działalności orzeczniczej i w codziennym funkcjonowaniu sądów, wskazując przy tym, że sąd jest administratorem danych osobowych zarówno osób w nim zatrudnionych, jak i tych, których dane pozyskuje w związku z prowadzonymi sprawami. Mówił także o roli GIODO w Systemie Informacyjnym Schengen, o tajemnicach zawodów prawniczych w kontekście uprawnień Policji i służb bezpieczeństwa państwa, a także wyjaśniał wątpliwości dotyczące przetwarzania danych osobowych m.in. na potrzeby wokand sądowych czy udzielania informacji publicznej. Przedstawił też praktyczne aspekty związane z zabezpieczeniem sprzętu informatycznego. Spotkanie to było również okazją do przybliżenia jego uczestnikom problematyki reformy unijnego prawa ochrony danych osobowych oraz stanowiska, jakie w tej sprawie zajęła Krajowa Rada Sądownicza.

W formule szkolenia przebiegały także warsztaty nt. obrotu wierzytelnościami na rynku polskim (17.04.2013 r.), podczas których przedstawiciel GIODO omówił zagadnienia związane z prawem do prywatności i ochrony danych osobowych stron tego procesu, podkreślając konieczność dookreślenia zakresu danych niezbędnych w procesie dochodzenia wierzytelności oraz wskazania warunków upubliczniania danych dłużników. Ponadto przedstawione zostało orzecznictwo sądów polskich w sprawach związanych z udostępnieniem danych osobowych w ramach obrotu wierzytelnościami.

Na uwagę zasługuje także spotkanie przedstawiciela GIODO z studentami Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego (12.12.2013 r.), podczas którego przedstawiciel GIODO omawiał zagadnienia z zakresu bezpieczeństwa baz danych w praktyce aptecznej w ramach przedmiotu Opieka Farmaceutyczna.

Niektóre ze szkoleń miały formę wideokonferencji, jak to zorganizowane przez Ministerstwo Administracji i Cyfryzacji dla przedstawicieli kadry kierowniczej, administratorów danych i Administratorów Bezpieczeństwa Informacji ze wszystkich urzędów wojewódzkich w Polsce, czy szkolenie e-learningowe dla pracowników Grupy EDF, które było zapowiedzią szkoleń zaplanowanych w spółkach tego podmiotu na nadchodzący 2014 rok. W formie szkolenia online przebiegało również spotkanie z przedsiębiorcami zorganizowane przez Polską Agencję Rozwoju Przedsiębiorczości.

2) Szkolenia wewnętrzne pracowników Biura GIODO

W zależności od dynamiki przyjmowania nowych pracowników do pracy w Biurze Generalnego Inspektora Ochrony Danych Osobowych, organizowane były szkolenia dla wszystkich nowo zatrudnionych 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 eduGIODO, status GIODO na tle organizacji i funkcjonowania organów władzy publicznej, organizacja i techniczne środki zabezpieczania danych, rejestracja zbiorów, podstawy prawne SIS, CIS i Europolu, europejskie standardy ochrony danych osobowych oraz przekazywanie danych do państw trzecich.

3) Udział pracowników Biura GIODO w szkoleniach organizowanych przez podmioty zewnętrzne

Pracownicy Biura GIODO korzystali ze szkoleń, warsztatów i seminariów informatycznych, które miały na celu podnoszenie ich kompetencji w zakresie zarządzania i administrowania posiadaną infrastrukturą informatyczną. W sumie odbyło się 15 takich spotkań. Wśród najważniejszych znalazły się seminaria i konferencje szkoleniowe, np. „IT Breakfast for GOV" Fundacji IT Leader Club Polska, dedykowany dla liderów IT z administracji publicznej i centralnej (23.01.2013), seminarium PIIT „Jakość systemów i rozwiązań informatycznych (15.02.2013), szkolenie „Jak zmienić rolę działów informatyki

w jednostkach sektora publicznego?" (13.06.2013) zorganizowane przez Zakład Zarządzania Informatyką w Instytucie Informatyki i Gospodarki Cyfrowej Szkoły Głównej Handlowej, szkolenie z zarządzania nowym systemem operacyjnym urządzeń FortiGate (6.09.2013), szkolenie ABW pt. „Bezpieczeństwo, administracja i zarządzanie systemami Microsoft Windows Serwer 2008 oraz nowości dotyczące bezpieczeństwa w Microsoft Windows Serwer 2012" (30-31.12.2013) czy szkolenie dla administracji rządowej i samorządowej nt. bezpieczeństwa i zarządzania systemami Microsoft 7 oraz nowości dotyczące bezpieczeństwa w Microsoft Windows 8, którego organizatorem był Rządowy Zespół Reagowania na Incydenty Komputerowe. Szkolenia te oferowane są w ramach współpracy Agencji Bezpieczeństwa Wewnętrznego z firmą Microsoft w zakresie bezpieczeństwa teleinformatycznego SCP (Security Cooperation Program).

8.2.5. Konkursy

W analizowanym 2013 r. Generalny Inspektor Ochrony Danych Osobowych był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

1. **Konkurs GIODO „Mam prawo do ochrony prywatności i danych osobowych"**

Generalny Inspektor Ochrony Danych Osobowych był organizatorem konkursu „Mam prawo do ochrony prywatności i danych osobowych", skierowanego do uczniów szkół podstawowych i gimnazjów objętych ogólnopolskim programem edukacyjnym GIODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Celem konkursu było wyłonienie laureatów, którzy wykazują się wiedzą i kreatywnością z zakresu tematyki konkursu i przygotują najciekawsze prace literackie, plastyczne lub multimedialne z zakresu prawa do prywatności i ochrony danych osobowych. Prace laureatów oraz wybranych uczestników konkursu zostały zaprezentowane 3 czerwca 2013 r. na wystawie podczas seminarium podsumowującego 3. edycję ogólnopolskiego programu edukacyjnego oraz podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, która odbywała się w dniach 23-26 września 2013 r. w Warszawie.

2. **Konkurs na esej pt. „Profilowanie klientów dla celów działań marketingowych".**

Przygotowanie eseju stanowiącego rozwiązanie kazusu z zakresu ochrony danych osobowych wykorzystywanych do profilowania klientów dla celów działań marketingowych, było przedmiotem 3. 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. Konkurs miał na celu propagowanie wśród studentów polskich uczelni, wiedzy z zakresu ochrony danych osobowych, umożliwienie im sprawdzenia swojej wiedzy w tej dziedzinie prawa, a także promowanie tych, którzy posiadają umiejętność formułowania praktycznych rozwiązań w zetknięciu z problemami prawnymi. Zwycięzcy otrzymali – oprócz nagród rzeczowych – także nagrody specjalne w postaci możliwości odbycia praktyk zawodowych w Biurze Generalnego Inspektora Ochrony Danych Osobowych. Uroczystość wręczenia nagród odbyła się w dniu 22 maja 2013 r. na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie podczas V Konferencji Naukowej „Bezpieczeństwo w Internecie: Internet – granice jawności".

3. Konkurs dla sklepów internetowych „Bezpieczny eSklep 2013"

Celem 3. edycji konkursu dla sklepów internetowych „Bezpieczny eSklep 2013" było wyróżnienie najbardziej wiarygodnych i rzetelnych sklepów internetowych w Polsce i tym samym podniesienie jakości i bezpieczeństwa usług handlu elektronicznego. Organizatorem Konkursu był Instytut Logistyki i Magazynowania z siedzibą w Poznaniu. Konkurs, wraz z towarzyszącą mu akcją „Kupuj bezpiecznie w Internecie", objęty został honorowym patronatem Generalnego Inspektora Ochrony Danych Osobowych. Kapituła Konkursu - w skład której wszedł Zastępca Generalnego Inspektora Ochrony Danych Osobowych - oceniała sklepy m.in. w zakresie zgodności z prawem zapisów regulaminów sklepów, obsługi procesu zakupu, sposobu zabezpieczania danych osobowych, czytelności strony internetowej, opisów oferowanych towarów, stosowania zasad dobrych praktyk gospodarczych, opinii konsumentów, a także możliwości sprzedaży poza granice Polski

4. Konkurs na najciekawsze inicjatywy edukacyjne oraz Złote Pióro Programu

Celem konkursu zorganizowanego przez Generalnego Inspektora Ochrony Danych Osobowych było promowanie najciekawszych inicjatyw mających na celu upowszechnienie

wiedzy o ochronie danych osobowych i prawa do prywatności wśród uczniów i nauczycieli - uczestników i partnerów metodycznych III edycji ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Placówki wyróżnione w konkursie uhonorowane zostały nie tylko nagrodami rzeczowymi. Generalny Inspektor Ochrony Danych Osobowych wyróżnił ponadto laureata I miejsca statuetką tzw. „Złotym Piórem Programu" za pracę na rzecz upowszechniania wiedzy o ochronie danych osobowych, prowadzoną w ramach ww. programu. Ponadto Ministerstwo Administracji i Cyfryzacji przyznało jedno dodatkowe wyróżnienie za najbardziej inspirującą inicjatywę edukacyjną, a Kuratorium Oświaty w Warszawie wyróżniło trzy placówki oświatowe za najciekawsze inicjatywy edukacyjne podejmowane na terenie województwa mazowieckiego.

Uroczystość wręczenia nagród odbyła się w dniu 3 czerwca 2013 r. w Warszawie, podczas seminarium podsumowującego III edycję programu. Spotkanie to było okazją do wymiany doświadczeń i omówieniu dobrych praktyk przez laureatów konkursu z uczestnikami programu.

5. Ogólnopolski Konkurs „Prawo a Nowe Technologie"

Studenckie Koło Naukowe – Blok Prawa Komputerowego działające na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej byli organizatorami ogólnopolskiego konkursu „Prawo a Nowe Technologie", który objęty został patronatem Generalnego Inspektora Ochrony Danych Osobowych. Zadanie konkursowe polegało na napisaniu eseju dotyczącego wpływu współczesnych rozwiązań technologicznych na ewolucję prawa. Konkurs na najlepszy artykuł swoim zakresem tematycznym obejmował kwestie związane z prawem nowych technologii, w szczególności dotyczące prawnych aspektów przetwarzania danych, handlu elektronicznego, zagadnień informatyki prawniczej, prawa telekomunikacyjnego, ochrony danych osobowych, własności intelektualnej w kontekście technologii informacyjnych, przestępczości komputerowej, prawnych aspektów stosowania technologii informacyjnych w zarządzaniu podmiotami prywatnymi, sprawowaniu władzy publicznej, w wymiarze sprawiedliwości, a także zagadnień pokrewnych. Adresatami konkursu byli studenci publicznych i niepublicznych uczelni wyższych.

8.2.6. Projekty i programy

W roku sprawozdawczym 2013, 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 przez GIODO od 2009 r. pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka. Ponadto w 2013 r. rozpoczęta została realizacja nowego europejskiego projektu o nazwie PHAEDRA, finansowanego ze środków Komisji Europejskiej.

I. Unijne projekty partnerskie

a) W latach 2012-2013 Biuro GIODO kontynuowało realizację III edycji projektu mobilności finansowanego z środków Unii Europejskiej w ramach Programu Leonardo da Vinci będącego częścią ww. Programu „Uczenia się przez całe życie". Celem tego projektu było 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 odbywanie stażu: w urzędzie Rady Europy (Council of Europe), u Europejskiego Rzecznika Ochrony Danych (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. 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 był w okresie od 1 czerwca 2012 r. do 30 grudnia 2013 r.

b) W analizowanym roku sprawozdawczym Biuro GIODO kontynuowało rozpoczęty w 2012 r. projekt partnerski finansowany 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 był 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.

Inspiracją do przygotowania 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.

Projekt ukierunkowany jest 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.

II. Projekt PHAEDRA

Konsorcjum złożone z czterech partnerów z Belgii, Zjednoczonego Królestwa, Hiszpanii oraz Polski zainicjowało nowy europejski projekt, którego celem jest pomoc organom ochrony danych w usprawnieniu egzekwowania przepisów w zakresie ochrony prywatności. Dwuletni projekt badawczy o nazwie PHAEDRA rozpoczął się 22 stycznia 2013 r. spotkaniem partnerów w siedzibie Vrije Universiteit Brussel w Brukseli. Projekt ten współfinansowany jest przez Unię Europejską (Dyrekcję Generalną Sprawiedliwości – DG Justice) w ramach programu Prawa Podstawowe i Obywatelstwo (Fundamental Rights and Citizensship – „Action grants"). PHAEDRA to akronim wyrażenia „Improving Practical and Helpful cooperAtion bEtween Data PRotection Authorities" („Usprawnienie praktycznej i przydatnej współpracy miedzy organami ochrony danych"). Cztery instytucje partnerskie to Vrije Universiteit Brussel (Belgia) – koordynator projektu, Trilateral Research & Consulting (Zjednoczone Królestwo), Generalny Inspektor Ochrony Danych Osobowych (Polska) oraz Universitat Jaume I (Hiszpania).

Zasadniczym zamierzeniem projektu jest zdiagnozowanie problemów utrudniających współpracę i koordynację działań między poszczególnymi organami ochrony danych osobowych (DPAs), rzecznikami ds. ochrony prywatności (PCs), organami ds. egzekwowania ochrony danych osobowych i prywatności (PEAs) oraz innymi podmiotami zajmującymi się

problematyką prawa do prywatności i ochrony danych osobowych. Następnym krokiem będzie przygotowanie rekomendacji zmierzających do poprawy tej sytuacji. W efekcie projekt przyczyni się do poprawy współpracy i koordynacji działań między wszystkimi zainteresowanymi stronami w zapewnieniu rzeczywistej ochrony danych osobowych.

Pierwsze warsztaty projektu PHAEDRA odbyły się 24 września 2013 r. w Warszawie podczas 35. Międzynarodowej Konferencji Rzeczników Danych Osobowych i Prywatności, której gospodarzem był Generalny Inspektor Ochrony Danych Osobowych.

III. Krajowy program edukacyjny

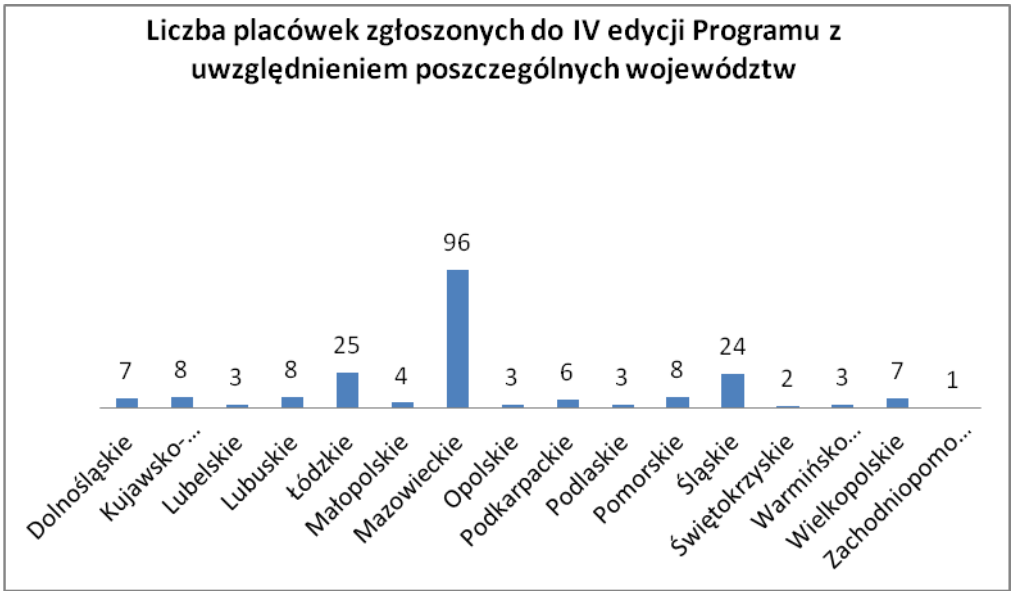
W 2013 r. kontynuowany był **ogólnopolski program edukacyjny „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli**". Podstawowym celem programu jest poszerzenie oferty edukacyjnej szkół o treści związane z ochroną danych osobowych i prawem do prywatności, poprzez zwiększenie wiedzy nauczycieli, pedagogów szkolnych i uczniów o zagadnienia związane z tą tematyką. Program ten jest przedsięwzięciem realizowanym pod honorowym patronatem Minister Edukacji Narodowej i Rzecznika Praw Dziecka od 2009 r. Uczestnicy programu - nauczyciele i metodycy – 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.

Mając na uwadze dotychczasowe pozytywne doświadczenia związane z realizacją programu w okresie do 2011 roku, gdy był on skierowany wyłącznie do szkół gimnazjalnych, w minionym roku sprawozdawczym 2012 podjęta została decyzja o jego rozszerzeniu na szkoły podstawowe i ponadgimnazjalne. Dla uczestników programu rok 2013 rozpoczął się organizacją w placówkach oświatowych obchodów VI Dnia Ochrony Danych Osobowych pod hasłem „Twoje dane – twoja sprawa". W ramach tego święta szkoły zorganizowały konkursy dla uczniów (wiedzy, plastyczne, multimedialne), quizy, apele, przedstawienia autorskie z zakresu ochrony danych osobowych z udziałem dzieci i młodzieży oraz wizyty w urzędach miast i gmin, prokuraturze i sądzie. Ponadto uczniowie wzięli udział w grach miejskich oraz happeningach, podczas których rozdawali przechodniom ulotki informujące o prawie każdego do prywatności i dotyczących go danych osobowych.

W dniu 3 czerwca 2013 r. odbyło się seminarium podsumowujące 3. edycję programu w latach 2012/2013, podczas którego wyróżniono szkoły i placówki oświatowe wyłonione w konkursie GIODO na najciekawsze inicjatywy edukacyjne z zakresu prawa do prywatności i ochrony danych osobowych.

Natomiast uroczysta inauguracja IV edycji programu w roku szkolnym 2013/2014 odbyła się w dniach 24-25 października 2013 roku, konferencją szkoleniową pt. „ABC Ochrony Danych Osobowych, zorganizowaną w Warszawie pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka. Podczas tego spotkania przedstawione zostały główne założenia programu oraz prezentacje ekspertów Biura GIODO. Dotyczyły one w szczególności genezy ochrony danych, zasad przetwarzania danych osobowych w placówkach oświatowych, rejestracji zbiorów danych osobowych oraz praktycznych wskazówek będących wynikiem przeprowadzonych przez GIODO kontroli w szkołach. Sesja pn. „Dobre praktyki liderów Programu" była okazją do wymiany doświadczeń oraz poglądów m.in. z prekursorami i liderami tego przedsięwzięcia, na temat metodyki prowadzenia zajęć o ochronie danych osobowych i prawie do prywatności oraz organizowania różnych akcji, jak gry miejskie, pikniki rodzinne czy konkursy. Natomiast drugi dzień szkolenia miał charakter warsztatowy. Uczestnikom zaprezentowane zostały przykłady, jak zorganizować w szkole Dzień Ochrony Danych Osobowych w oparciu o różne typy gier, jak rozmawiać z dziećmi i młodzieżą o bezpieczeństwie w sieci oraz wyjaśniano, o co chodzi w ochronie prywatności i danych osobowych i jak można skutecznie dochodzić swoich praw. Uczestnicy konferencji otrzymali materiały edukacyjne zawierającą scenariusze lekcji. W szkoleniu wzięło udział ponad 150 osób reprezentujących 139 placówek zgłoszonych do IV edycji programu.

W rezultacie, w 2013 roku do programu przystąpiło 208 placówek oświatowych z 16 województw, w tym 96 szkół podstawowych, 67 gimnazjów, 36 szkół ponadgimnazjalnych i 9 placówek doskonalenia zawodowego nauczycieli. Spośród zgłoszonych do programu placówek 161 przystąpiło do niego po raz pierwszy. Partnerami IV edycji programu byli: Gliwicki Ośrodek Metodyczny, Śląska Sieć Metropolitarna Sp. z o.o. oraz Ośrodek Edukacji Informatycznej i Zastosowań Komputerów.



Wykres 38: ***Liczba placówek oświatowych zgłoszonych do IV edycji Programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli" z podziałem na poszczególne województwa.***

8.2.7. Konferencje, seminaria, spotkania

W roku sprawozdawczym 2013, Generalny Inspektor Ochrony Danych Osobowych organizował konferencje i seminaria, jak również brał aktywny udział w konferencjach zorganizowanych przez inne podmioty. Aktywnie uczestniczył w różnych wydarzeniach, w tym również w tych organizowanych cyklicznie, jak chociażby obchody Światowego Dnia Społeczeństwa Informacyjnego w Polsce w 2013 r., czy Tydzień Zapobiegania Kradzieży Tożsamości oraz patronował długofalowym przedsięwzięciom, jak chociażby portal informacyjny „Bezpieczna Chmura", którego twórcą i realizatorem jest polski oddział stowarzyszenia Cloud Security Alliance Polska. W 2013 r. Generalny Inspektor Ochrony Danych Osobowych objął swoim patronatem 42 wydarzenia zorganizowane przez różne podmioty, których wykaz znajduje się w załączniku nr 6.

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 trzy

tego rodzaju przedsięwzięcia – w 2012 roku w Dąbrowie Górniczej i Krakowie oraz w 2013 roku w Poznaniu.

Poniżej przedstawione zostały przykłady najważniejszych wydarzeń krajowych o charakterze ogólnopolskim lub międzynarodowym z udziałem Generalnego Inspektora bądź przedstawicieli jego Biura. Ich pełny wykaz zawiera załącznik nr 7.

1. Wykład otwarty w Szkole Głównej Handlowej (Warszawa, 18.01.2013 r.)

„Ocena wpływu usługi chmurowej na ochronę prywatności - Privacy Impact Assesment (PIA)" to tytuł wykładu otwartego, wygłoszonego 18 stycznia 2013 r. przez dra Wojciecha R. Wiewiórowskiego, GIODO, w Szkole Głównej Handlowej w Warszawie. Wykład odbywał się w ramach promocji studiów podyplomowych „Zastosowanie technologii *cloud computingu* w modelu biznesowym", które zostały uruchomione w roku akademickim 2012/2013. W wystąpieniu GIODO przedstawił aspekty związane z ochroną prywatności i danych osobowych w kontekście efektywnego wykorzystywania technologii chmurowych w nowoczesnych modelach biznesu. Organizatorem tego wydarzenia była Katedra Systemów Zarządzania w Kolegium Nauk o Przedsiębiorstwie Szkoły Głównej Handlowej w Warszawie.

2. II Obchody Dnia Ochrony Informacji Niejawnych (Dąbrowa Górnicza, 22.01.2013)

Po raz drugi w Polsce odbyły się obchody Dnia Ochrony Informacji Niejawnych, ustanowionego w rocznicę uchwalenia ustawy o ochronie informacji niejawnych. Inicjatorem ustanowienia święta, obchodzonego w przededniu Europejskiego Dnia Ochrony Danych Osobowych, było Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Na spotkaniu tym utworzona została nowa ogólnopolska organizacja o nazwie Stowarzyszenie Wspierania Bezpieczeństwa Narodowego (SWBN). Podczas sesji tematycznej wystąpił Zastępca Generalnego Inspektora Ochrony Danych Osobowych.

3. VII Dzień Ochrony Danych Osobowych – 28 stycznia 2013 r.

W dniu 28 stycznia 2013 r. Generalny Inspektor Ochrony Danych Osobowych już po raz siódmy organizował Europejski Dzień Ochrony Danych Osobowych ustanowiony przez Komitet Ministrów Rady Europy. W tym dniu świętowana jest bowiem rocznica otwarcia do podpisu Konwencji Nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Wydarzenia związane

z VII Dniem Ochrony Danych Osobowych odbywały się zarówno w Brukseli, jak i we wszystkich stolicach państw członkowskich Unii Europejskiej.

Wydarzenia związane z VII Dniem Ochrony Danych Osobowych odbywały się przez cały tydzień, zarówno w kraju, jak i za granicą. Z tej okazji w Warszawie zorganizowany został Dzień Otwarty, na który złożyła się konferencja, wykłady ekspertów, konkursy, konferencje prasowe, a pracownicy Biura GIODO udzielali bezpłatnych porad prawnych i konsultacji z zakresu ochrony danych osobowych. Osoby zainteresowane mogły otrzymać publikacje Generalnego Inspektora Ochrony Danych oraz inne materiały edukacyjne dotyczące prawa do prywatności i ochrony danych osobowych. Temat przewodni VII Dnia Ochrony Danych Osobowych brzmiał „Dane osobowe w ochronie zdrowia i w badaniach klinicznych" i pod takim samym tytułem odbywała się ww. konferencja naukowa. Uczestnikami tego wydarzenia byli eksperci zajmujący się problematyką danych medycznych i ich ochroną, w tym przedstawiciele administracji publicznej, środowiska lekarskiego, świata nauki i biznesu. Konferencja podzielona została na trzy sesje tematyczne. Pierwsza z nich dotyczyła tajemnic prawnie chronionych oraz tego, co ta ochrona oznacza dla systemów IT, druga – systemów informatycznych w ochronie zdrowia, zaś tematem ostatniej sesji były zagadnienia ochrony prywatności w badaniach klinicznych. Podczas konferencji Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład pt. „Europejskie ramy ochrony danych osobowych a prawo polskie".

Obchodom VII Dnia Ochrony Danych Osobowych towarzyszyły również wydarzenia za granicą. W Brukseli zaplanowano okolicznościowe spotkanie z europejskimi rzecznikami ochrony danych, a także wykład GIODO dla eurodeputowanych.

4. II Łódzki Konwent Informatyków (Spała, 5.02.2013 r.)

Prawne aspekty zarządzania dokumentacją elektroniczną, informatyczny system zarządzania oświatą, bezpieczeństwo danych elektronicznych w administracji publicznej w kontekście ostatniego etapu ich przetwarzania, czyli usuwania, tworzenie ewidencji miast, ulic i adresów oraz kwestia wdrożenia elektronicznego systemu zarządzania dokumentacją, to tylko kilka przykładów tematów poruszanych podczas II Łódzkiego Konwentu Informatyków, który odbył się w dniach 5-6 lutego 2013 r. w Spale. Podczas Konwentu dr Wojciech R. Wiewiórowski, GIODO, wygłosił wykład pt. „Administracja publiczna w chmurach. Ochrona prywatności przy przenoszeniu realizacji zadań publicznych do modelu Iaas i SaaS", w którym poruszył istotne zagadnienia związane z najnowocześniejszymi technologiami IT

i możliwościami ich zastosowania w administracji publicznej. Organizatorem Konwentu był magazyn „IT w Administracji", natomiast patronat nad tym wydarzeniem objęli: Generalny Inspektor Ochrony Danych Osobowych, Ministerstwo Administracji i Cyfryzacji, Marszałek Województwa Łódzkiego oraz Urząd Komunikacji Elektronicznej. Uczestnikami Konwentu byli przedstawiciele łódzkich instytucji, urzędnicy, prawnicy i naukowcy zajmujący się tematyką IT oraz przedstawiciele firm komercyjnych dostarczających rozwiązania technologiczne dla sektora publicznego. Spotkanie w Spale to był pierwszy z cyklu 10 Konwentów Informatyków miesięcznika „IT w Administracji", które pod patronatem GIODO odbyły się w 2013 roku.

5. 2. Kongres Wolności w Internecie (Warszawa, 13.02.2013 r.)

Ministerstwo Administracji i Cyfryzacji było organizatorem spotkania poświęconego szansom i zagrożeniom, jakie niesie nowa cyfrowa rzeczywistość. Dyskusja wokół tego tematu koncentrowała się głównie na sposobach wspierania rozwoju gospodarki cyfrowej, prawie autorskim w społeczeństwie informacyjnym oraz polityce integracji cyfrowej. W panelu pn. „Prywatność w sieci – jakie znaczenie ma rozporządzenie o ochronie danych osobowych dla użytkowników?", Generalny Inspektor Ochrony Danych Osobowych podkreślał, jak ważna dla prywatności i poczucia bezpieczeństwa w sieci jest skuteczność w egzekwowaniu przepisów o ochronie danych osobowych, gdzie ich elastyczność ułatwia wszystkim użytkownikom bezpieczne załatwianie spraw przez Internet, natomiast przedsiębiorcom - wdrażanie i tworzenie nowych modeli biznesowych.

6. Międzynarodowa Konferencja ePSIplatform i Centrum Cyfrowego (Warszawa, 22.02.2013 r.)

Generalny Inspektor Ochrony Danych Osobowych był uczestnikiem międzynarodowej Konferencji poświęconej otwartości danych i ponownemu wykorzystaniu danych publicznych. Hasłem przewodnim tego spotkania było „Gotcha! – getting everyone on bard". Dane publiczne zawierają ogromną ilość informacji na temat działania administracji, ale mogą też dotyczyć indywidualnych obywateli. O tym, jak zapewnić bezpieczne i zgodne z prawem wykorzystanie danych osobowych, wyważyć kwestię otwartości danych w kontekście ochrony prywatności - opowiadał dr Wojciech R. Wiewiórowski, GIODO, podczas swojego wystąpienia charakteryzując m.in. zasadę *privacy by design.* Organizatorami

tego wydarzenia byli ePSIplatform oraz Centrum Cyfrowe przy współpracy Koła Naukowego CyberLaw Uniwersytetu Warszawskiego.

7. IV Forum Corporate Legal Counsel (Warszawa, 27-28.02.2013 r.)

Pod hasłem „Więcej niż doradztwo prawne!" odbywało się w Warszawie IV Forum Corporate Legal Counsel 2013. Celem tego dorocznego spotkania przedstawicieli środowiska prawników korporacyjnych, sektora publicznego i kancelarii prawnych było omówienie najważniejszych wyzwań, nowości oraz problemów, z którymi stykają się w swojej pracy przedstawiciele tej branży. Podczas Forum uczestnicy mieli okazję aktualizacji wiedzy na styku prawa i biznesu w takich dziedzinach, jak prawo o ochronie danych osobowych, prawo konkurencji, prawo pracy oraz prawo własności intelektualnej. Jednym z 29 prelegentów był Generalny Inspektor Ochrony Danych Osobowych, który podczas drugiego dnia Forum przedstawił prezentację pt. „Profilowanie osoby fizycznej w projekcie nowych ram prawnych ochrony danych osobowych w Unii Europejskiej". W wystąpieniu poruszył kwestie ryzyk związanych z przetwarzaniem danych osobowych, generalnej dopuszczalności profilowania, obowiązków profilującego wynikających z projektu rozporządzenia UE oraz z rekomendacji Rady Europy z 2010 r., a także zagadnienie oceny wpływu przedsięwzięcia na ochronę danych osobowych. Patronat nad IV Forum Corporate Legal Counsel 2013 – Forum Dyrektorów Prawnych, sprawowali: Krajowa Izba Radców Prawnych oraz Polskie Stowarzyszenie Prawników Przedsiębiorstw.

8. VI Konferencja SEMAFOR (Warszawa, 5-6.03.2013 r.)

VI Konferencja SEMAFOR 2013 – Security Management and Audit Forum, to jedna z największych konferencji poświęconych bezpieczeństwu informacji, audytu oraz zarządzaniu ryzykiem. Wśród tematów poruszanych podczas obrad wiele uwagi poświęconej zostało zagadnieniom związanym z ochroną danych osobowych w przedsiębiorstwie – jak radzić sobie w praktyce z zagadnieniami ochrony danych osobowych przy aktualnym stanie prawnym i dynamicznym rozwoju nowoczesnych technologii. Podczas Konferencji Generalny Inspektor Ochrony Danych Osobowych, wygłosił wykład pt. „Zabezpieczenia aplikacji webowych – dlaczego zbłądziliśmy", w którym przedstawił najważniejsze problemy związane z testami bezpieczeństwa tych aplikacji w kontekście wzrastającej skali zagrożeń. Organizatorami wydarzenia byli: magazyn Computerworld oraz stowarzyszenia ISSA Polska i ISACA Warsaw Chapter.

Honorowy patronat nad Konferencją sprawowali Generalny Inspektor Ochrony Danych Osobowych oraz European Network and Information Security Agency (ENISA).

9. Polski Kongres Prawa Farmaceutycznego i Ochrony Zdrowia (Warszawa, 14.03.2013 r.)

Zagadnienia, wokół których toczyły się obrady Polskiego Kongresu Prawa Farmaceutycznego i Ochrony Zdrowia „Allerhand summie: Pharma & Heath", dotyczyły najważniejszych obecnie problemów środowiska medycznego. Wśród nich znalazła się m.in. kwestia polityki refundacyjnej, wpływu działań NFZ i Ministra Zdrowia na funkcjonowanie podmiotów leczniczych czy stopień przygotowania Polski na wejście w życie Dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej. Kongres adresowany był do przedstawicieli sektora medycznego (w tym osób zarządzających podmiotami leczniczymi, reprezentantów środowiska aptekarskiego, przemysłu farmaceutycznego i wyrobów medycznych), ubezpieczeniowego oraz do prawników. Duże zainteresowanie uczestników Kongresu wzbudził panel dotyczący zarządzania danymi osobowymi w medycynie i branży ubezpieczeniowej, z uwzględnieniem ryzyka i odpowiedzialności związanej z dostępem do systemu eWUŚ i drugiej funkcjonalności wdrażanego systemu w postaci dostępu on-line do danych osobowych, odnoszących się pośrednio do stanu zdrowia ubezpieczonych. W ramach tego panelu dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, wygłosił referat pt. „Rola administratorów danych i przetwarzających w systemach informacyjnych zawierających dane osobowe". Organizatorem Kongresu była Fundacja Instytut Allerhanda.

10. 2. edycja Konferencji Naukowej pt. „Ataki sieciowe" (Toruń, 18-19.03.2013 r.)

Głównym tematem Konferencji, która pod honorowym patronatem GIODO odbyła się na Uniwersytecie Mikołaja Kopernika w Toruniu - były zagadnienia związane z cyberprzestępczością i atakami cyberprzestępców, z uwzględnieniem odpowiedzialności podmiotów, w szczególności korporacyjnych, za naruszanie prywatności i bezpieczeństwa danych osobowych. „Nieuprawnione udostępnienie smatrfonów i innych urządzeń mobilnych" – to tytuł wystąpienia Generalnego Inspektora Ochrony Danych Osobowych podczas tego wydarzenia. Organizatorami Konferencji byli: Studenckie Koło Naukowe Prawa

Nowych Technologii przy Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu.

11. Spotkanie GIODO z przedstawicielami Krajowej Izby Gospodarczej (Warszawa, 19.03.2013 r.)

W dniu 19 marca 2013 r. w siedzibie Krajowej Izby Gospodarczej (KIG) odbyło się spotkanie Prezydium Krajowej Izby i przedstawicieli niektórych izb regionalnych, którego tematem była ochrona danych osobowych w działalności podmiotów gospodarczych, a także najważniejsze założenia z projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływie tych danych. Na powyższe tematy wykład wygłosił Zastępca Generalnego Inspektora ochrony Danych osobowych. Omówione zostały też kwestie dotyczące współpracy GIODO z KIG w zakresie stosowania przepisów ochrony danych osobowych przez izby regionalne i bilateralne oraz podmioty gospodarcze w ich codziennej działalności. Wynikiem tej współpracy był zaplanowany na dzień 6 maja 2013 r. przez Wielkopolską Izbę Przemysłowo – Handlową przy udziale Poznańskiej Izby Rzemieślniczej i Zrzeszeń Handlowych, Sejmik Gospodarczy poświęcony ochronie danych osobowych w działalności podmiotów gospodarczych. Sejmik odbył się w ramach organizowanych przez GIODO w dniach 6 i 7 maja 2013 Dni Otwartych GIODO w Poznaniu.

12. Debata „Prywatność w nowych technologiach" (Warszawa, 20.03.2013 r.)

Granice prywatności we współczesnym świecie oraz adekwatność regulacji prawnych do zagrożeń bezpieczeństwa prywatności i danych osobowych, były tematem wystąpienia przedstawiciela GIODO, inaugurującego tę debatę. Podczas spotkania konfrontowani byli ze sobą dwaj specjaliści, reprezentujący odmienne poglądy na temat prawa do prywatności i ochrony danych osobowych w obliczu rozwoju nowoczesnych technologii. Dyskusje toczyły się wokół zagadnień ochrony prywatności w usługach świadczonych drogą elektroniczną, w serwisach społecznościowych, reklamie behawioralnej, a także ochrony przed naruszeniami. Głównym organizatorem debaty była Fundacja Bezpieczna Cyberprzestrzeń przy wsparciu interdyscyplinarnego Koła Naukowego badań nad Internetem i nowoczesnymi technologiami CyberLaw, które działa na Uniwersytecie Warszawskim. Patronat nad tym wydarzeniem objęli: Generalny Inspektor Ochrony Danych Osobowych, Polska Izba

Informatyki i Telekomunikacji, Krajowa Izba Radców Prawnych oraz Dziekan Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.

13. XII Krajowa Konferencja Szkoleniowa „Postępy w chorobach wewnętrznych – INTERNA 2013" (Warszawa, 5.04.2013 r.)

Zasadom przetwarzania danych osobowych w elektronicznej dokumentacji medycznej oraz gwarancjom przejrzystości systemu poświęcone było wystąpienie przedstawiciela GIODO podczas XII Krajowej Konferencji Szkoleniowej „Postępy w chorobach wewnętrznych – INTERNA 2013", która odbyła się w dniach 5-6 kwietnia w Warszawie. Blisko 3000 lekarzy, uczestników tego spotkania, skorzystało z wiedzy i doświadczenia przedstawiciela GIODO podczas sesji satelitarnej „Dokumentacja medyczna – czy jesteś gotowy na jej wdrożenie w wersji elektronicznej?", podczas której omówione zostały zagadnienia bezpieczeństwa danych osobowych w ochronie zdrowia w kontekście obowiązujących i przewidywanych zmian legislacyjnych wraz z oceną skutków regulacji określoną w projekcie rozporządzenia Parlamentu Europejskiego i Rady z dnia 25 stycznia 2012 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. W wystąpieniu przedstawiciela GIODO pt. „Ochrona danych osobowych w procesie wdrażania elektronicznej dokumentacji medycznej", omówione zostały podstawowe zasady ochrony danych osobowych pacjentów w odniesieniu do kwestii niezawodnej identyfikacji pacjentów określonej w art. 8 ust. 7 Dyrektywy 95/46/WE, a także systemu identyfikacji i uwierzytelniania pracowników opieki zdrowotnej i przypisanych im w systemie elektronicznym ról i funkcji. Organizatorem tego dorocznego wydarzenia medycznego było Towarzystwo Internistów Polskich oraz specjalistyczny portal internetowy Medycyna Praktyczna.

14. Konferencja „Dyrektor XXI wieku – mobilność, bezpieczeństwo, innowacyjność" (Mszczonów, 12-13.04.2013 r.)

Konferencja „Dyrektor XXI wieku – mobilność, bezpieczeństwo, innowacyjność" stała się miejscem spotkania dyrektorów szkół, którzy wykorzystują dzienniki elektroniczne nie tylko do dokumentowania przebiegu nauczania czy podnoszenia jakości kształcenia, ale również jako profesjonalne narzędzia wspierające dyrektora w zarządzaniu placówką oświatową. Tematyka konferencji dotyczyła zagadnień, z którymi boryka się współczesny dyrektor szkoły, m.in. ochrony i przetwarzania danych osobowych w placówkach oświatowych,

nowoczesnych technologii, public relations, prawa oświatowego oraz procesu zamiany dziennika papierowego na jego formę elektroniczną. Z chwilą wdrożenia w placówce systemów IT i idąca za tym zmiana sposobu przechowywania i przetwarzania danych osobowych, skutkują potrzebą przeformułowania dotychczasowych procedur organizacji pracy szkoły, a w szczególności zdefiniowania nowego zadania dyrektora placówki – jako administratora danych osobowych. Na te aspekty zarządzania szkołą wskazał w swoim wystąpieniu przedstawiciel GIODO. W swoim wystąpieniu przedstawił uczestnikom Konferencji skutki transformacji informatycznej, jakie zaszły we współczesnej szkole, w której bieżące wykorzystywanie Internetu, dzienników elektronicznych, portali społecznościowych oraz szeroko rozumianej technologii stało się standardem i wymusiło dostosowanie się do przepisów związanych z podstawowymi zasadami ochrony danych osobowych przetwarzanych w systemach informatycznych szkoły. Konferencja ta objęta została patronatem Generalnego Inspektora Ochrony Danych Osobowych, zaś jej organizatorami byli Firma LIBRUS oraz magazyn EduFakty – Uczę nowocześnie.

15. Warsztaty „Obrót wierzytelnościami na rynku polskim" (Warszawa, 17.04.2013 r.)

Pytaniom związanym z prawidłowym obrotem wierzytelnościami na rynku polskim poświęcona była 2. edycja warsztatów dla przedstawicieli branży windykacyjnej, zorganizowanych przez Business Media Solutions. Podczas tego spotkania przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych, w referacie pt. „Ochrona danych osobowych a bezpieczeństwo obrotu wierzytelnościami" przedstawił uczestnikom podstawowe zagadnienia związane z prawem do prywatności i ochrony danych osobowych stron tego procesu. Wśród najważniejszych kierunków tej ochrony zasygnalizowano konieczność dookreślenia zakresu danych niezbędnych w procesie dochodzenia wierzytelności świetle zasad ochrony danych osobowych oraz wskazanie warunków upubliczniania danych osobowych dłużników, w szczególności zaś tych danych, które są objęte tajemnicami prawnie chronionymi. Duże zainteresowanie słuchaczy wzbudziła część wykładu, w której prezentowane zostało orzecznictwo sądów polskich w sprawach związanych z udostępnianiem danych osobowych w ramach obrotu wierzytelnościami.

16. **II Warmińsko - Mazurski Konwent Informatyków (Wilkasy k/Giżycka, 18.04.2013)**

Głównym tematem II Warmińsko – Mazurskiego Konwentu Informatyków były m.in. zagadnienia dotyczące bezpieczeństwa danych elektronicznych przy tworzeniu i utrzymaniu

systemów informacyjnych administracji publicznej, prawne aspekty wykorzystania chmury obliczeniowej oraz usługi e-administracji dla przedsiębiorców. Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład pt. „Administracja publiczna w chmurach. Ochrona prywatności przy przenoszeniu realizacji zadań publicznych do modelu Iaas i SaaS", w którym zapoznał uczestników Konwentu z definicją przetwarzania danych w chmurze, wskazując przy tym na pięć głównych cech przetwarzania chmurowego, a także omówił podstawowe modele: Iaas, PaaS oraz SaaS. W swoim wystąpieniu wskazał, że tylko dalsze studia nad „privacy by design" i technologiami zwiększającymi prywatność (privacy-enhancing technologies), połączone z rozpoznawaniem różnic w implementacji europejskich zasad ochrony danych osobowych w poszczególnych krajach członkowskich, może nas przybliżyć do rozwiązania problemów prawnych i organizacyjnych, jakie *cloud computing* napotyka w Europie. W opinii polskiego organu ds. ochrony danych osobowych, drogą do budowania sprawnego i zaufanego rynku przetwarzania danych w chmurze stanowią również działania samoregulacyjne podejmowane przez grupy przedsiębiorców oraz wiążące reguły korporacyjne (binding corporate rules) ustanawiane przez dostarczyciela chmury.
II Warmińsko – Mazurski Konwent Informatyków odbywał się pod patronatem Generalnego Inspektora Ochrony Danych Osobowych, zaś jego organizatorem był miesięcznik „IT w Administracji".

17. Konferencja „Bezpieczeństwo sieci Smart Grid" (Warszawa, 7.05.2013 r.)

Podstawowy model systemów energetycznych przechodzi obecnie głęboką przemianę. Dzięki technologii teleinformatycznej przeistoczył się ze względnie prostego układu dostawca-odbiorca, w układ zbliżony do rozproszonej sieci komputerowej o wielostronnym przepływie energii i informacji. Dlatego tematyka cyfryzacji systemów zarządzania dystrybucją i przesyłem, a także zagadnienia związane z zagrożeniami oraz metodami ich usuwania, stały się głównym tematem obrad tej Konferencji. Podczas tego spotkania przedstawiciel Generalnego Inspektora Danych Osobowych omówił prawne i techniczne aspekty związane z funkcjonowaniem sieci typu *smart grid*. Podkreślił przy tym, że rozwój tych sieci dotyka podstawowych praw obywatelskich, których ochronę gwarantuje art. 47 i 51 Konstytucji RP. Tymczasem przy pomocy danych zebranych przez inteligentne liczniki i dokonanej na ich podstawie analizy schematów zachowań, można w łatwy sposób opracować profil osobowy ich użytkownika. Dlatego trzeba sobie jasno zdawać sprawę, że zarówno na etapie tworzenia

prawa dla tych systemów, jak i stosowania go w praktyce, kwestie związane z ochroną prywatności powinny stanowić priorytet. Konferencja ta była jednym z wielu przedsięwzięć, które odbywały się w ramach obchodów Światowego Dnia Społeczeństwa Informacyjnego 2013, której organizatorem było Polskie Towarzystwo Informatyczne. W Komitecie Honorowym tego wydarzenia zasiadał dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych.

18. V Konferencja Naukowa pt. „Internet – granice jawności" (Warszawa, 22.05.2013)

Budowaniu zaufania do technologii cyfrowych poprzez zapewnienie ochrony prywatności i danych osobowych poświęcona była 5 edycja Konferencji Naukowej z cyklu „Internet – granice jawności", która odbyła się na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Podczas swojego wystąpienia Generalny Inspektor Ochrony Danych Osobowych wskazywał na potrzebę pilnego uregulowania kwestii przetwarzania danych osobowych przez podmioty gospodarcze, powtórnego wykorzystywania ogólnie dostępnych danych i informacji, w szczególności w kontekście zakresu, w jakim publiczne rejestry mogą być ze sobą łączone, a informacje w nich zawarte wykorzystywane przez sektor prywatny. Sygnalizowany też był problem nieostrych znaczeniowo pojęć stanowiących podstawę odmowy udzielenia informacji, które zawarte są m.in. w ustawie o dostępie do informacji publicznej, jak np. „prywatność", „osoba pełniąca funkcję publiczną" czy „ważny interes państwowy". Prowadzi to bowiem do rozbieżności interpretacyjnych i tym samym do różnych rozstrzygnięć wydawanych przez sądy. Organizatorami tego wydarzenia byli: GIODO, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Naukowe Centrum Prawno-Informatyczne, Naczelny Sąd Administracyjny, Ministerstwo Administracji i Cyfryzacji, Ministerstwo Sprawiedliwości, Urząd Komunikacji Elektronicznej oraz Agencja Bezpieczeństwa Wewnętrznego.

19. IX Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych (Bielsko-Biała, 27-29.05.2013 r.)

Praktyczne aspekty funkcjonowania pionów ochrony informacji oraz zmiany w prawie ochrony danych osobowych to jedne z głównych tematów IX Kongresu Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Przedstawiciele Państwowej Inspekcji Pracy omówili tematykę współpracy z Generalnym Inspektorem Ochrony Danych Osobowych w zakresie podniesienia skuteczności działań na rzecz przestrzegania przepisów

o ochronie danych osobowych w stosunkach pracy, wynikającą z podpisania porozumienia w sprawie zasad współdziałania PIP i GIODO. Podczas tego spotkania zastępca Generalnego Inspektora Ochrony Danych Osobowych wygłosił wystąpienie poświęcone roli Inspektora Ochrony Danych (ABI) w firmie/instytucji w kontekście reformy unijnych przepisów dotyczących ochrony danych osobowych. Obradom towarzyszyły także praktyczne pokazy i prezentacje nowoczesnych technik, technologii i urządzeń dla zapewnienia bezpieczeństwa informacji i danych osobowych. Organizatorami IX Kongresu Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych były: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych (KSOIN) oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego (SWBN). Patronat honorowy nad tym wydarzeniem sprawowali Generalny Inspektor Ochrony Danych Osobowych, Rzecznik Praw Obywatelskich, Krajowa Izba Gospodarcza, Polska Konfederacja Pracodawców Prywatnych Lewiatan i Międzynarodowe Targi Poznańskie.

20. Międzynarodowa Konferencja Naukowa „Techniczne Aspekty Przestępczości Teleinformatycznej" (Szczytno, 28-29.05.2013 r.)

Konferencja poświęcona była najnowszym trendom w cyberprzestępczości w kontekście zapewnienia bezpieczeństwa elektronicznym transakcjom płatniczym, monitorowaniu zagrożeń w Internecie oraz omówieniu specyfiki pracy przy zwalczaniu oszustw w sieci w kontekście ujawniania, pozyskiwania, zabezpieczania i prezentacji dowodów cyfrowych. Konferencja była też okazją do wymiany doświadczeń oraz metod i narzędzi wspomagających zwalczanie cyberprzestępczości. Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład na temat „Karnych i administracyjno-karnych regulacji nowych ram ochrony danych osobowych w Unii Europejskiej".

W konferencji uczestniczyło ponad 200 specjalistów w dziedzinie przestępczości internetowej z całego świata, w tym z Chin, Australii i Stanów Zjednoczonych. Organizatorem tego wydarzenia był Instytut Badań nad Przestępczością Kryminalną i Terroryzmem Wydziału Bezpieczeństwa Wewnętrznego Wyższej Szkoły Policji w Szczytnie we współpracy z Grupą Allegro.

21. Seminarium podsumowujące 3. edycję ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli" (Warszawa, 3.06.2013 r.)

Przedstawieniu i omówieniu inicjatyw edukacyjnych podejmowanych w 2013 r. przez uczestników 3. edycji ogólnopolskiego programu „Twoje dane – twoja sprawa …" , poświęcone było seminarium, którego organizatorem był Generalny Inspektor Ochrony Danych Osobowych. Podczas tego spotkania, Generalny Inspektor Ochrony Danych Osobowych, Ministerstwo Administracji i Cyfryzacji oraz Kuratorium Oświaty w Warszawie, wyróżniło placówki oświatowe, które opracowały najciekawsze i najbardziej inspirujące działania edukacyjne.

22. **Konferencja MCSS'13 (Kraków, 7.06.2013 r.)**

Systemy audiowizualne i bezpieczeństwo usług multimedialnych były tematem Konferencji „Multimedia Communications, Services and Security", której organizatorem była Katedra Telekomunikacji Akademii Górniczo-Hutniczej w Krakowie. Podczas tego wydarzenia prezentowane były kwestie związane z bezpieczeństwem mobilnych i bezprzewodowych sieci dostępowych usług multimedialnych, w ramach wsparcia dla Siódmego Programu Ramowego (7PR) badań nad bezpieczeństwem. Podstawowym zadaniem Konferencji była prezentacja nowoczesnych rozwiązań technicznych na rzecz wsparcia cywilnych rozwiązań bezpieczeństwa dla zapewnienia ochrony przed zagrożeniami (np. terroryzm czy klęski żywiołowe), przy jednoczesnym poszanowaniu prawa do prywatności i ochrony danych osobowych. Znaczna część wystąpień dotyczyła również projektu INDECT i koncentrowała się na omówieniu prawnych aspektów monitoringu (wizyjnego, Internetu, usług), równoległego przetwarzania dźwięku i obrazu, aplikacji biometrycznych, itp. w celu zapewnienia optymalnego wykorzystania tych nowoczesnych technologii dla celów związanych z zapewnieniem porządku publicznego. W sesji dotyczącej prawa do prywatności i ochrony danych osobowych, przedstawiciel GIODO wygłosił referat pt. „Dilemmas of privacy protection in researches on public security. Data Protection Authority's point of view", w którym przedstawił stanowisko organu ds. ochrony danych osobowych w najważniejszych kwestiach prawnych i etycznych, dotyczących badań nad bezpieczeństwem publicznym.

23. **Forum Sekretarzy Województwa Kujawsko-Pomorskiego (Białe Błota, 13.06.2013)**

W spotkaniu z sekretarzami województwa kujawsko-pomorskiego, poświęconym ochronie danych osobowych, uczestniczył zastępca Generalnego Inspektora Ochrony Danych Osobowych. Podczas wykładu omówił zagadnienie ochrony danych osobowych i informacji niejawnych w praktyce administracji publicznej, podstawowe zasady wynikające z ustawy o ochronie danych osobowych oraz kwestię pozyskiwania i udostępniania danych osobowych tzw. zwykłych i szczególnie chronionych, w tym z rejestrów publicznych. Część wykładu poświęcona była kwestii bezpieczeństwa danych osobowych i środków, jakie należy stosować w dobie rozwoju nowych technologii i społeczeństwa informacyjnego. Ważnym elementem tego wystąpienia była prezentacja zasad i założeń reformy unijnych przepisów o ochronie danych osobowych. Organizatorami spotkania były Kujawsko-Pomorski oddział Fundacji Rozwoju Demokracji Lokalnej oraz Gmina Białe-Błota.

24. **III Europejski Kongres Małych i Średnich Przedsiębiorstw (Katowice, 16.09.2013)**

Kwestie ładu gospodarczego i jego znaczenia dla małych i średnich firm w dobie kryzysu były głównym tematem obrad podczas III Europejskiego Kongresu MŚP, który pod nazwą „*Współpraca i kooperacja firm sektora MŚP w wymiarze regionalnym, krajowym i międzynarodowym"* odbywał się w Katowicach. Podczas Kongresu omawiane były m.in. tematy dotyczące zmian w ustawodawstwie, finansowania rozwoju inwestycji, wsparcia Unii Europejskiej dla polskich przedsiębiorców, roli konkurencyjności, innowacji i nowych technologii w sektorze MŚP. Przedsiębiorcy debatowali także na temat roli kobiet w europejskiej gospodarce, w szczególności w obliczu zmian, które pozwolą im odgrywać większą rolę w przedsiębiorstwach. Zaprezentowane też zostały wyniki badań PARP pt. „Panel Polskich Przedsiębiorstw" dotyczący skutków spowolnienia gospodarczego dla MŚP. Natomiast w drugim dniu Kongresu odbyła się uroczysta sesja Sejmiku Województwa Śląskiego z udziałem Rady Krajowej Izby Gospodarczej i Rad Regionalnych Izb Gospodarczych. W gronie ekspertów sesji plenarnej poświęconej bezpieczeństwu informacji „Ochrona informacji niejawnych, biznesowych, danych osobowych, własności intelektualnej i przemysłowej. Biała Księga Bezpieczeństwa Narodowego RP", zasiadał Zastępca Generalnego Inspektora Ochrony Danych Osobowych. W swoim wystąpieniu pt. „Ochrona danych u przedsiębiorcy" podkreślił wagę dotyczącą zapewnienia bezpieczeństwa danych osobowych w działalności firm, w celu podniesienia ich społecznego wizerunku i tym samym

zwiększenia konkurencyjności na rynku. Organizatorem tego wydarzenia była Regionalna Izba Gospodarcza w Katowicach.

25. **Ogólnopolska Konferencja Naukowo-Szkoleniowa „IT w zdrowiu – zmiany w sektorze zdrowia 2014 i prognoza 2014-2010" (Gliwice, 18.09.2013 r.)**

Najnowsze rozwiązania w dziedzinie technologii informatycznych oraz współczesne osiągnięcia techniki w branży usług medycznych, zostały zaprezentowane podczas Konferencji oraz towarzyszących jej targów. Przedmiotem Konferencji były zaplanowane na najbliższe lata rozwiązania w dziedzinie wykorzystania nowoczesnych technologii w obszarze usług medycznych, które wynikają ze strategii zmian w systemie ochrony zdrowia w latach 2012-2015. Wśród tematów poruszanych podczas tego wydarzenia znalazły się zagadnienia związane z przygotowaniem się placówki do wdrożenia elektronicznej dokumentacji medycznej, bezpieczeństwo danych medycznych, podniesienie jakości obsługi pacjenta poprzez m.in. wdrożenie sieci bezprzewodowej, efektywne i bezpieczne zarządzanie majątkiem szpitala, digitalizacja dokumentacji medycznej, itp. Podczas sesji plenarnej Konferencji, zastępca Generalnego Inspektora Ochrony Danych Osobowych, w wystąpieniu pt. „Przetwarzanie danych osobowych w służbie zdrowia w związku z wprowadzeniem elektronicznej dokumentacji medycznej", przedstawił podstawowe zasady ochrony danych przetwarzanych w dokumentacji placówek służby zdrowia.

26. **LXII Seminarium z cyklu Akademia Prawa Komputerowego (Warszawa, 19.09.2013 r.)**

Problematyka prawna zwalczania bezprawnych treści w Internecie była głównym tematem obrad podczas LXII Seminarium z cyklu Akademia Prawa Komputerowego pt. „Bezprawne treści w Internecie - analiza orzecznictwa polskich organów i sądów oraz TSUE", którego organizatorem było Centrum Promocji Informatyki. Przedstawiono tu szereg istotnych orzeczeń wydanych zarówno przez Trybunał Sprawiedliwości UE, jak i sądy krajowe, w tym sądy polskie, dotyczących ochrony własności intelektualnej oraz dóbr osobistych. W orzeczeniach tych widoczne były wysiłki sądów w kwestii ustalenia zakresu obowiązków dostawców treści i pośredników internetowych w zwalczaniu naruszeń praw użytkowników i osób trzecich w Internecie. W bloku poświęconym prawnym aspektom przygotowywania postępowań sądowych, w szczególności pozyskiwania danych osobowych sprawców naruszeń, a także obowiązków dostawców treści i pośredników internetowych w zakresie

przekazywania sądom materiałów na potrzeby tych postępowań i realizacji wydanych już orzeczeń, przedstawiciel GIODO wygłosił referat pt. „Udostępnianie danych osobowych na potrzeby postępowań cywilnych". W wystąpieniu tym zarysowany został tryb i warunki udostępniania danych osobowych dla potrzeb wszczęcia postępowania przed sądami powszechnymi, w szczególności kwestie związane z zakresem ujawnianych danych i odpowiedzialnością administratorów, natomiast na przykładzie wybranych rozstrzygnięć sądów administracyjnych, przybliżone zostały zagadnienia związane z udostępnianiem danych osobowych w świetle ochrony tajemnic prawnie chronionych.

27. I Jesienny Konwent Ochrony Danych i Informacji (Łódź, 2.10.2013 r.)

Zasady udostępniania danych osobowych w kontekście ograniczeń w tym zakresie w odniesieniu do informacji udzielanych w trybie dostępu do informacji publicznej, wymagania i zagrożenia związane z prowadzeniem działalności z wykorzystaniem mediów elektronicznych, zagadnienia rejestracji zbiorów danych z poprzez platformę eGIODO oraz bezpieczeństwo danych osobowych w działalności leczniczej - to tylko przykłady zagadnień, które były poruszane podczas 1 Jesiennego Konwentu Ochrony Danych Osobowych i Informacji, który odbył się 2 października 2013 r. w Łodzi. Jest to już drugie tego rodzaju wydarzenie zorganizowane na terenie województwa łódzkiego, a jego adresatami byli przede wszystkim przedstawiciele jednostek samorządu terytorialnego, służby zdrowia i spółdzielczości mieszkaniowej. W ten sposób Firma Forsafe, organizator Konwentu, zapoczątkowała cykliczne spotkania z różnymi środowiskami w celu przybliżenia tematyki ochrony danych osobowych i informacji. Podczas tego wydarzenia, przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych w referacie pt. *„Zasady realizacji skarg na przetwarzanie danych osobowych a tajemnice prawnie chronione"* przybliżył zagadnienia związane z przebiegiem postępowania w sprawach skargowych i stosowaniem procedury administracyjnej przed GIODO.

28. XV Forum Monitoringu Polskiego (Pułtusk, 4.10.2013 r.)

Kiedy nagranie z monitoringu stanowi zbiór danych osobowych, po spełnieniu jakich warunków można wykorzystywać kamery w zakładzie pracy oraz temu, jak prowadzić monitoring w przestrzeni publicznej, poświęcone było wystąpienie Generalnego Inspektora Ochrony Danych Osobowych „Monitoring wizyjny a prawna ochrona prywatności" podczas XV edycji Forum Monitoringu Polskiego. Spotkanie to poświęcone było aktualnym aspektom

prawno-normatywnym oraz trendom technicznym monitoringu bezpieczeństwa obiektów. Uczestniczyli w nim zarówno przedstawiciele instytucji zainteresowanych instalacją takich systemów, m.in. banków, wojska, agencji ochrony osób i mienia, jak i firm wykonawczych. Organizatorem wydarzenia, nad którym GIODO sprawował patronat honorowy, było Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM".

29. Konferencja Naukowa „Ochrona publicznych baz danych" (Sobolewo, 6.11.2013 r.)

Ochrona danych osobowych przetwarzanych w publicznych bazach danych była tematem wystąpienia przedstawiciela GIODO podczas Konferencji „Ochrona publicznych baz danych", której organizatorem był Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie. Konferencja odbywała się w ramach projektu badawczo-rozwojowego, realizowanego na rzecz bezpieczeństwa i obronności państwa „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", współfinansowanego ze środków Narodowego Centrum Badań i Rozwoju.

30. XVII Kongres Administratorów Bezpieczeństwa Informacji (Chlewiska, 13-14.11.2013 r.)

XVII Kongres ABI pt. „Sieć Skutecznych Rozwiązań" poświęcony był szczególnej roli Administratora Bezpieczeństwa Informacji wobec zagadnień ochrony danych w usługach internetowych oraz innych wybranych zagadnieniach przetwarzania danych osobowych. Omówione i przedyskutowane zostały bardzo istotne praktyczne problemy związane z realizacją zgodnego z prawem przetwarzania przez pracodawców danych osobowych pracowników, powierzenia przetwarzania danych oraz analizy ryzyka przetwarzania danych osobowych w chmurze obliczeniowej. Wykład wprowadzający pt. „Rola ABI jako instytucji ochrony danych osobowych w zmieniających się uwarunkowaniach przetwarzania danych" wygłosił Generalny Inspektor Ochrony Danych Osobowych. Organizatorem tego wydarzenia był European Network Security Institute (ENSI).

31. Dolnośląski Konwent Informatyków (Jugowice, 21-22.11.2013 r.)

To już kolejna edycja wydarzenia organizowanego cyklicznie w różnych regionach Polski przez magazyn „IT w Administracji". Konwent stanowi platformę wymiany doświadczeń oraz wiedzy na temat zagadnień IT oraz ich zastosowania w administracji publicznej. Eksperci rozmawiali m.in. na temat dobrych praktyk w zarządzaniu działem informatyki,

elektronicznych skrzynkach podawczych, wykorzystaniu nowoczesnych technologii w kontekście oszczędności w sektorze publicznym i bezpieczeństwa informacji oraz weryfikacji zabezpieczeń sieci jednostki za pomocą narzędzi open source. Natomiast Generalny Inspektor Ochrony Danych Osobowych przedstawił prawne aspekty wykorzystania chmury obliczeniowej w administracji publicznej. Patronat nad tym wydarzeniem objęli: Generalny Inspektor Ochrony Danych Osobowych, Ministerstwo Gospodarki, Ministerstwo Administracji i Cyfryzacji, Centrum Projektów Informatycznych oraz Urząd Komunikacji Elektronicznej.

8.2.8. Porozumienia o współpracy

Uniwersytet Ekonomiczny w Poznaniu i Generalny Inspektor Ochrony Danych Osobowych podpisali w dniu 7 maja 2013 r. porozumienie o współpracy.

Uroczyste podpisanie porozumienia miało miejsce przed rozpoczęciem konferencji naukowej „Prawne i ekonomiczne aspekty przetwarzania danych osobowych" będącej centralnym punktem III Dnia Otwartego GIODO w Poznaniu.

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.

8.2.9. Inne informacje

a) Powołanie Rady Naukowej GIODO

Zgodnie z §3 ust. 3 Statutu Biura Generalnego Inspektora Ochrony Danych Osobowych, stanowiącego załącznik do rozporządzenia Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 225, poz. 1350) w Biurze mogą działać Rada Naukowa i Komisje Ekspertów, których skład określa Generalny Inspektor.

Według Regulaminu Organizacyjnego Biura GIODO członków Rady powołuje Generalny Inspektor na okres swojej kadencji spośród osób naukowo zajmujących się zagadnieniami objętymi działalnością Rady i wyróżniających się wiedzą w tym zakresie. Pracami Rady

kieruje jej przewodniczący. Do zadań Rady Naukowej należy: zajmowanie stanowisk w sprawach przedstawionych przez Generalnego Inspektora, analizowanie problemów ochrony danych osobowych i przedstawianie w tym zakresie Generalnemu Inspektorowi wyników swoich prac oraz inicjowanie działań na rzecz rozwoju ochrony danych osobowych, w tym prac naukowo-badawczych i wydawniczych.

Na podstawie wspomnianych aktów w 2013 r. Generalny Inspektor powołał Radę Naukową, w skład której wchodzą: dr hab. Paweł Fajgielski, (prof. Katolickiego Uniwersytetu Lubelskiego) – przewodniczący, dr Grzegorz Sibiga (Instytut Nauk Prawnych Polskiej Akademii Nauk) – wiceprzewodniczący, dr Arwid Mednis (Uniwersytet Warszawski), dr Ewa Perłakowska (Naczelna Dyrekcja Archiwów Państwowych), prof. dr hab. Jakub Stelina (Uniwersytet Gdański), prof. dr hab. Grażyna Szpor (Uniwersytet Kardynała Stefana Wyszyńskiego), dr inż. Janusz Zawiła-Niedźwiecki (Politechnika Warszawska) oraz prof. dr hab. Teresa Górzyńska z Instytutu Nauk Prawnych Polskiej Akademii Nauk, która zmarła 7 kwietnia 2013 r.

b) Aktualizacja poradnika GIODO i UKE dla użytkowników telekomunikacyjnych

W związku ze zmianami przepisów prawa, Generalny Inspektor Ochrony Danych Osobowych dokonał aktualizacji „Poradnika dla użytkowników publicznie dostępnych usług telekomunikacyjnych', opublikowanego w 2010 r. Publikacja ta powstała we współpracy Generalnego Inspektora Ochrony Danych Osobowych z Urzędem Komunikacji Elektronicznej[400].

c) Szerokie Porozumienie na Rzecz Umiejętności Cyfrowych

W dniu 3 lipca 2013 r. – z inicjatywy Ministra Administracji i Cyfryzacji oraz Lidera Cyfryzacji w Polsce – zostało powołane Szerokie Porozumienie na Rzecz Umiejętności Cyfrowych, nad którym patronat honorowy sprawuje Prezydent RP Bronisław Komorowski. Generalny Inspektor Ochrony Danych Osobowych jest członkiem Komitetu Honorowego tego Porozumienia, którego celem jest inspirowanie, wspieranie, popularyzowanie, inicjowanie i podejmowanie wszelkich działań na rzecz powszechnej edukacji cyfrowej i uświadamianie korzyści, jakie ona daje. Komitet Honorowy Szerokiego Porozumienia na Rzecz Umiejętności Cyfrowych jest ciałem doradczym, opiniującym strategiczne kierunki

[400] http://www.uke.gov.pl/poradnik-dla-uzytkownikow-uslug-telekomunikacyjnych-12791

realizacji celów Porozumienia, powoływanym na okres 2 lat. Przewodniczącym Komitetu Honorowego jest minister właściwy do spraw informatyzacji lub osoba przez niego wskazana.

d) Partnerstwo dla zwiększenia świadomości obywateli na rzecz cyfrowej tożsamości

Z inicjatywy UPC Polska oraz Ministerstwa Administracji i Cyfryzacji zostało powołane Partnerstwo dla zwiększenia świadomości obywateli na rzecz cyfrowej świadomości. Podstawowym zadaniem tego podmiotu jest budowa świadomości i zaufania pomiędzy przedsiębiorcami, administracją i internautami w celu najpełniejszego wykorzystania potencjału gospodarki cyfrowej. Partnerstwo działa w 3 grupach roboczych: ds. badań, ds. komunikacji obywatelskiej oraz ds. dobrych praktyk. Generalny Inspektor Ochrony Danych Osobowych jest członkiem każdej z tych grup. Partnerstwo rozpoczęło pracę 30 października 2013 r. w Warszawie, debatą poświęconą roli podnoszenia świadomości i wiedzy obywateli w zakresie zarządzania prywatnością w sieci w budowaniu zaufania do gospodarki cyfrowej. Cele Partnerstwa mają być realizowane m.in. poprzez nagłaśnianie w debacie publicznej kwestii zarządzania prywatnością w sieci, upowszechnianie dobrych praktyk ułatwiających dostęp do wiedzy w zakresie zarządzania danymi, a także edukowanie konsumentów i przedsiębiorców na temat zarządzania danymi w Polsce. Oprócz Generalnego Inspektora Ochrony Danych Osobowych Partnerstwo wspierają m.in.: Związek Pracodawców Branży Internetowej IAB Polska, Związek Banków Polskich, Fundacja Dobra Sieć, Onet.pl, Orange, a także Szerokie Porozumienie na rzecz Umiejętności Cyfrowych.

e) Grupa robocza ds. projektu zintegrowanego monitoringu zdarzeń na tle rasistowskim i ksenofobicznym, przy Radzie ds. Przeciwdziałania Dyskryminacji Rasowej, Ksenofobii i związanej z nimi Nietolerancji

W dniu 15 kwietnia 2013 r. - pod przewodnictwem Ministra Administracji i Cyfryzacji - rozpoczęła pracę Rada ds. Przeciwdziałania Dyskryminacji Rasowej, Ksenofobii i związanej z nimi Nietolerancji, powołana zarządzeniem nr 6 Prezesa Rady Ministrów z dnia 13 lutego 2013 r. Głównym zadaniem Rady jest zapewnienie koordynacji działań organów administracji rządowej oraz ich współdziałania z organami samorządu terytorialnego i innymi podmiotami, w zakresie przeciwdziałania i zwalczania dyskryminacji rasowej, ksenofobii i związanej z nimi nietolerancji. Na drugim posiedzeniu Rady w dniu 20 maja 2013 r. powołana została grupa robocza, której celem jest stworzenie projektu zintegrowanego monitoringu zdarzeń na tle rasistowskim i ksenofobicznym, w postaci elektronicznej platformy, na której rejestrowane

będą ww. zdarzenia oraz monitorowane postępy w prowadzeniu spraw z tego zakresu przez organy ścigania i wymiaru sprawiedliwości. W składzie tej grupy znaleźli się przedstawiciele Ministerstwa Spraw Wewnętrznych, Prokuratury Generalnej, Ministerstwa Sprawiedliwości, Helsińskiej Fundacji Praw Człowieka, Stowarzyszenia „Nigdy Więcej" oraz Generalnego Inspektora Ochrony Danych Osobowych.

f) V edycja kampanii edukacyjnej „Nie daj się okraść, chroń swoją prywatność"

Kampania ta miała na celu edukację społeczeństwa w zakresie ochrony danych osobowych i zwrócenie uwagi na zjawisko tzw. kradzieży tożsamości. W ramach tej akcji prowadzona była ankieta internetowa, na stronie www.ochronatozsamosci.pl, dzięki której każdy mógł sprawdzić, w jakim stopniu chroni swoje dane i co powinien w swoim zachowaniu zmienić, by ustrzec się przed ich kradzieżą. Ankieta miała również na celu zwrócenie uwagi na odpowiednie przechowywanie i niszczenie dokumentów w pracy i w domu. Szczegółowe wyniki badań zaprezentowane zostały podczas konferencji prasowej PAP z udziałem Generalnego Inspektora Ochrony Danych Osobowych oraz Prezesa Biura Informacji Kredytowej. Dodatkowo odbyły się wykłady GIODO na wybranych warszawskich uczelniach. Głównym organizatorem akcji była firma Fellowes.

g) Internetowa lista publikacji z zakresu ochrony danych osobowych

Na stronie www.giodo.gov.pl zamieszczona została lista publikacji dotyczących szeroko pojętej tematyki ochrony danych osobowych. Każdy zainteresowany pomocą przy tworzeniu tej listy, proszony jest o przysyłanie zgłoszeń na specjalnym formularzu. Nadsyłane publikacje są cennym uzupełnieniem wykazu literatury przedmiotu, który może być przydatny dla każdego, kto zajmuje się tymi zagadnieniami. Uwzględnienie konkretnej pozycji na liście publikacji nie oznacza, że jest ona szczególnie polecana. Intencją GIODO było jedynie stworzenie wykazu literatury przedmiotu, w którym znajdą się zarówno starsze – powstałe przed laty - publikacje, jak i te najnowsze. W sumie wykaz ten obejmuje 305 pozycji za lata 1972-2013.

9. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych

Jednym z zadań Generalnego Inspektora Ochrony Danych Osobowych jest uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. Zadanie to realizowane jest przede wszystkim poprzez udział GIODO 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 działań Generalnego Inspektora prowadzonych w ramach współpracy międzynarodowej, należy udział w posiedzeniach 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, której jest założycielem i w której pełni rolę Sekretariatu – 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 jest członkiem Komitetu Konsultacyjnego ds. Konwencji Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (T-PD) i aktywnie uczestniczy w pracach tego podmiotu. W latach 2011-2013 prace Komitetu T-PD koncentrowały się w szczególności na modernizacji Konwencji Nr 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. Podczas 30. posiedzenia, które odbyło się w dniach 15-18 października 2013 r., dokonana została analiza projektu Raportu wyjaśniającego do Konwencji Nr 108, poproszono Sekretariat o wprowadzenie zasygnalizowanych w dyskusjach zmian do tego dokumentu, który następnie został przedłożony Komitetowi Ad Hoc ds. Ochrony Danych (CAHDATA), odpowiedzialnemu za zakończenie prac nad Raportem i prowadzonymi równolegle pracami nad projektem modernizowanej Konwencji.

Inne ważne zadania stojące przed polskim organem ds. ochrony danych w ramach współpracy międzynarodowej, związane są z jego udziałem w pracach grup koordynujących nadzór nad SIS II, VIS, CIS oraz IMI, grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac, Systemem Informacji Celnej, a także Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji (tzw. Grupa Berlińska). Ponadto, Generalny Inspektor bierze aktywny udział w pracach Wspólnego Organu Nadzorczego nad Europolem (Joint Supervisory Body of Europol - JSB Europol)[401], a także Wspólnego Organu Nadzorczego właściwego w sprawach ochrony danych osobowych w związku z wykorzystaniem systemu informacyjnego dla odpraw celnych (Joint Supervisory Authority Customs - JSA Customs)[402].

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

W omawianym roku sprawozdawczym 2013, podobnie jak w latach poprzednich, Generalny Inspektor Ochrony Danych Osobowych uczestniczył w cyklicznie odbywających się spotkaniach **Grupy Roboczej Art. 29 ds. ochrony danych osobowych** (GR Art. 29) organizowanych w Brukseli. GR Art. 29 ustanowiona została na podstawie art. 29 dyrektywy 95/46/WE. W jej skład wchodzą po jednym przedstawicielu z każdego państwa członkowskiego UE, Europejski Inspektor Ochrony Danych Osobowych oraz przedstawiciel Komisji Europejskiej.

Do zadań GR Art. 29[403] należy badanie wszelkich kwestii dotyczących stosowania krajowych środków przyjętych na mocy ww. dyrektywy (by przyczyniać się do jednolitego stosowania tych środków), przekazywanie Komisji Europejskiej opinii na temat stopnia ochrony prywatności i danych osobowych we Wspólnocie i w państwach trzecich, doradzanie Komisji w sprawie proponowanych zmian tejże dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i swobód osób fizycznych w zakresie

[401] Więcej informacji na temat JSB Europol jest dostępnych na stronie internetowej: http://europoljsb.consilium.europa.eu/about.aspx?lang=pl

[402] 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.

[403] Art. 30 ust. 1 dyrektywy 95/46/WE.

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 również w odniesieniu do sektora łączności elektronicznej[404].

Podczas pierwszego w 2013 r., 89. posiedzenia Grupy Roboczej Art. 29 w dniach 26-27 lutego 2013 r. kontynuowane były prace dotyczące reformy ochrony danych, których rezultatem było oświadczenie podsumowujące dyskusję nad pakietem legislacyjnym w sprawie reformy ochrony danych osobowych w Unii Europejskiej. Przyjęta została Opinia 1/2013 stanowiąca dalszy wkład w dyskusję nad projektem dyrektywy o ochronie danych osobowych przetwarzanych przez organy policyjne i sądowe w sprawach karnych. Na obecnym etapie prac nad projektem tego dokumentu, GR Art. 29 postanowiła skoncentrować się na czterech kwestiach, które są obecnie uznawane za najważniejsze. Obejmują one wykorzystanie danych osób niebędących podejrzanymi, prawa osób, których dane dotyczą, stosowanie oceny skutków w zakresie ochrony prywatności oraz uprawnienia organów ochrony danych, zwłaszcza w odniesieniu do informacji poufnych lub niejawnych.

W porządku obrad 89 posiedzenia znalazła się również kwestia polityki prywatności Google. W tej sprawie Grupa Robocza Artykułu 29 zwróciła uwagę na braki w polityce prywatności Google oraz przedstawiła zalecenia dotyczące sposobu zaradzenia im. Zważywszy na fakt, że firma Google nie podjęła żadnych konkretnych środków w odpowiedzi na te zalecenia - i nadal nie były spełnione wymogi dyrektywy 95/46/WE – kontynuowane było dochodzenie w tej sprawie, koordynowane przez zespół roboczy pod przewodnictwem francuskiego organu ochrony danych (CNIL).

Z kolei w Opinii 2/2013 przedstawione zostało stanowisko Grupy odnośnie aplikacji na urządzenia inteligentne (27.02.2013 r.). W dokumencie tym omówiono ramy prawne mające zastosowanie do przetwarzania danych osobowych w trakcie opracowywania, dystrybucji i wykorzystywania aplikacji do urządzeń inteligentnych, ze szczególnym uwzględnieniem wymagania dotyczącego zgody, zasad w zakresie ograniczenia celu i minimalizacji danych, potrzeby podjęcia odpowiednich środków bezpieczeństwa, obowiązku prawidłowego informowania użytkowników końcowych, przestrzegania ich praw oraz rozsądnych okresów przechowywania. Zwrócono także uwagę na konieczność uczciwego przetwarzania danych

[404] Art. 15 ust. 3 dyrektywy 2002/58/WE.

pozyskanych od dzieci oraz dotyczących dzieci. Chodzi tu przede wszystkim o powstrzymanie się od przetwarzanie danych dzieci na potrzeby reklamy behawioralnej. Grupa robocza zaleciła opracowanie i wdrożenie prostego, skutecznego narzędzia dostępu online dla użytkowników, bez gromadzenia dodatkowych nadmiernych danych osobowych. Ważne jest bowiem, aby gromadzone i przetwarzane były tylko te dane, które są spójne z kontekstem, w jakim dostarczył je użytkownik aplikacji.

GR Art. 29 wypowiedziała się również w sprawie współpracy dotyczącej systemów przekazywania danych pomiędzy Europą a regionem Azji i Pacyfiku. W wydanym dokumencie (26.03.2013 r.) stanowiącym podsumowanie spotkania przedstawicieli Grupy Roboczej Artykułu 29 z przedstawicielami Wspólnoty Gospodarczej Azji i Pacyfiku (APEC), które odbyło się w Dżakarcie, przedstawiono narzędzia ułatwiające przekazywanie danych osobowych dla międzynarodowych przedsiębiorstw prowadzących działalność zarówno w Europie, jak i w regionie Azji i Pacyfiku. O ile w Unii Europejskiej mamy Wiążące Reguły Korporacyjne (BCR) regulujące międzynarodowe przekazywanie danych przez przedsiębiorstwa lub grupy przedsiębiorstw, to członkowie APEC opracowali własny systemem Zasad Transgranicznej Ochrony Prywatności (CBPR), służący ochronie danych osobowych w całym regionie Azji i Pacyfiku. Podobnie jak system BCR, system CBPR ma zapewnić, aby polityki prywatności przedsiębiorstw spełniały standardy ochrony danych osobowych. Zarówno system BCR UE, jak i system CBPR APEC, oparte są na tym samym podejściu, czyli na wykorzystaniu wewnętrznych wiążących reguł transgranicznego przekazywania danych osobowych, po ich wcześniejszym zatwierdzeniu przez organy ochrony danych UE lub przez specjalistów ds. rozliczalności uznanych przez APEC. GR Art. 29 przeprowadziła ostatnio badanie systemu CBPR celem określenia różnic i podobieństw z systemem BCR. Wykorzystując to wstępne porównanie jako punkt wyjścia, GR Art. 29 oraz zaangażowane gospodarki APEC podjęły działania zmierzające do znalezienia wspólnego punktu odniesienia dla tych międzynarodowych przedsiębiorstw, które prowadzą działania związane z gromadzeniem i/lub przetwarzaniem danych zarówno w Unii Europejskiej, jak i w regionie APEC[405].

[405] W dniu 31 stycznia 2013 r. odbyło się pierwsze spotkanie tzw. Komitetu BCR/CBPR mające na celu omówienie tego tematu. Wśród uczestników z UE znaleźli się przedstawiciele francuskiego organu ochrony danych (CNIL), niemieckiego Federalnego Rzecznika Ochrony Danych i Wolności Informacji, Europejskiego Inspektora Ochrony Danych oraz Komisji Europejskiej.

Ponadto przyjęta też została Opinia 3/2013 w sprawie ograniczenia celu ((2.04.2013 r.), która zawiera wskazania dla zgodnego z prawem przetwarzania danych, poprzez wyraźne wskazanie celu ich pozyskania oraz braku zgody na przetwarzanie niezgodne z tymi celami, np. na potrzeby przyszłych (niedookreślonych) celów administratora.

Z kolei 90 posiedzenie plenarne GR Art. 29 (16.04.2013 r.) przebiegało w formule spotkania europejskich organów ochrony danych z Julie Brill, Komisarz Federalnej Komisji Handlu USA (FTC). Federalna Komisja Handlu jest dla GR Art. 29 ważnym rozmówcą w kwestiach dotyczących ochrony prywatności w Stanach Zjednoczonych, jak również kluczowym partnerem w zakresie egzekwowania tego prawa. Komisarz Julie Brill poinformowała Grupę Roboczą o ostatnich działaniach FTC w obszarze ochrony prywatności, podkreślając zwłaszcza działania Komisji w odniesieniu do brokerów danych i aplikacji mobilnych. Poinformowała również o zrewidowanej ustawie o ochronie dzieci on-line, której wejście w życie miało nastąpić z dniem 1 lipca 2013 r. Ponadto po przyjęciu opinii w sprawie „ograniczenia celu", Grupa Robocza – jak zapowiedziała w swoim Programie prac na lata 2012/2013 – skoncentrowała się na innym kluczowym przepisie dotyczącym ochrony danych, a mianowicie na „uzasadnionych interesach administratora". Celem opracowywanej opinii GR Art. 29 było wyjaśnienie pojęcia „uzasadnionego interesu" oraz opracowanie praktycznych wskazówek, jak oszacować i osiągnąć równowagę między prawem do prywatności i ochrony danych osobowych podmiotu danych a interesami administratora, który będzie je przetwarzał. Podczas tego posiedzenia Grupa Robocza podjęła też decyzję o wysłaniu do Międzynarodowego Zrzeszenia Przewoźników Powietrznych (IATA) pism dotyczących oceny wpływu na ochronę prywatności, która miała być podjęta w odniesieniu do kontroli przyszłego projektu, oraz opracowania tzw. projektu NDC (New Distribution Capability), z którym wiąże się gromadzenie danych osobowych klientów linii lotniczych w celu oferowania klientom spersonalizowanych cen.

W dniu 22 kwietnia 2013 r. przyjęta została Opinia 04/2013 w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci (WP 205).

Inteligentne systemy pomiarowe i inteligentne sieci mają na celu umożliwienie produkcji, dystrybucji i wykorzystania energii w sposób inteligentny i racjonalny. Inteligentne systemy pomiarowe stanowią ważne elementy składowe inteligentnej dwukierunkowej sieci

elektrycznej, w której informacje pochodzące od użytkowników sieci są łączone w celu m.in. planowania zaopatrzenia w energię elektryczną w sposób bardziej efektywny i opłacalny. Ale zdaniem ekspertów upowszechnienie inteligentnych systemów pomiarowych umożliwi również gromadzenie, na masową skalę, danych osobowych z poszczególnych gospodarstw domowych oraz śledzenie zachowań domowników, na przykład poprzez rejestrację z jakich towarów i urządzeń najczęściej korzystają, jak wyglądają ich codzienne zajęcia, aktywność, jakie mają przyzwyczajenia, warunki czy styl życia. Dzięki tym informacjom możliwe będzie profilowanie konsumentów. Zastosowanie inteligentnych sieci i inteligentnych systemów pomiarowych generuje więc nowy obszar ryzyka dla prywatności i ochrony danych osobowych, np. w obszarze dyskryminacji cenowej, profilowania reklamy behawioralnej, podatków czy bezpieczeństwa domowego. Co więcej, czynniki ryzyka mogą wzrosnąć w przyszłości, biorąc pod uwagę coraz większą dostępność danych z innych źródeł, takich jak dane określające położenie geograficzne, dane dostępne poprzez śledzenie i profilowanie w Internecie, systemy nadzoru wideo czy systemy identyfikacji radiowej (RFID), z którymi dane z inteligentnych pomiarów mogą być łączone.

Proponowana ocena skutków w zakresie ochrony danych ma pomóc konsumentom, administratorom danych, organom ochrony danych, organom regulacji energetyki, organizacjom ochrony konsumentów i innym zainteresowanym stronom, w uzyskaniu wglądu w określone aspekty ochrony danych w aplikacjach inteligentnych pomiarów i inteligentnych sieci oraz w zidentyfikowaniu zarówno najlepszych praktyk, jak i ewentualnych docelowych obszarów wysokiego ryzyka na potrzeby kontroli. Dlatego była ona przedmiotem szczególnej uwagi europejskich organów ochrony danych zrzeszonych w GR Art. 29, którzy dokonali szczegółowej analizy szablonu oceny skutków w zakresie ochrony danych, zwracając uwagę przede wszystkim na: brak przejrzystości co do charakteru i celów oceny skutków w zakresie ochrony danych, błędy metodologiczne (np. poprzez częste utożsamianie czynników ryzyka z zagrożeniami) oraz brak identyfikacji i dopasowania czynników ryzyka właściwych dla danej branży i – co za tym idzie – uniemożliwienie zastosowanie odpowiednich środków kontroli służących ich ograniczeniu.

Ponadto europejskie organy ochrony danych przyjęły 19 kwietnia 2013 r. dokument wyjaśniający w sprawie wiążących reguł korporacyjnych (Binding Corporate Rules – BCR) dla przetwarzających, określonych w dokumencie roboczym 2/2012 (WP 195) z dnia 6 czerwca 2012 r. Wiążące reguły korporacyjne dla przetwarzających, wprowadzone w dniu 1

stycznia 2013 r. to wewnętrzne kodeksy postępowania dotyczące ochrony i bezpieczeństwa danych mające na celu zapewnienie, aby przekazywanie danych osobowych poza obszar Unii Europejskiej przez przetwarzającego, który działa w imieniu swoich klientów i wedle ich instrukcji, będzie odbywało się zgodnie z przepisami UE o ochronie danych. W związku z tym BCR dla przetwarzających należy rozumieć jako odpowiednie zabezpieczenia zapewnione przez przetwarzającego dla administratora, aby umożliwić mu wykazanie przed organem ochrony danych, odpowiedniej ochrony i uzyskania - gdy wymagają tego przepisy krajowe - niezbędnej zgody na przekazywanie danych osobowych do różnych podmiotów przetwarzających (np. podprzetwarzających oraz centrów danych).

Przedmiotowy dokument należy traktować jako zdecydowany krok GR Art. 29 mający na celu podkreślenie możliwości stosowania wiążących reguł korporacyjnych dla przetwarzających na podstawie podejścia samoregulacyjnego oraz współpracy między organami, bez uszczerbku dla możliwości stosowania innych narzędzi w odniesieniu do przekazywania danych osobowych za granicę, takich jak – w stosownych przypadkach – standardowe klauzule umowne lub zasady bezpiecznego transferu danych osobowych.

Natomiast w kwestii dotyczącej profilowania, GR Art. 29 przyjęła dokument doradczy[406], w którym opowiada się za wprowadzeniem wyraźnych ograniczeń wobec profilowania osób (28.05.2013 r.). Dokument ten stanowi jednocześnie dalszy wkład do dyskusji na temat reformy ochrony danych osobowych w UE. Europejskie organy ochrony danych uważają bowiem za niezbędne zawarcie w ogólnym rozporządzeniu o ochronie danych jasnej definicji profilowania, proponując zmianę treści art. 20 rozporządzenia poprzez: rozszerzenie zakresu przepisu i objęcie nim gromadzenia i tworzenia profili jako takich, zapewnienie przejrzystości poprzez zagwarantowanie osobom dodatkowych praw do informacji oraz wyższego poziomu kontroli, wzmocnienie rozliczalności i odpowiedzialności administratorów danych poprzez ustanowienie określonych zabezpieczeń w celu ochrony praw osób, których dane dotyczą (tj. obowiązek anonimizacji i pseudonimizacji danych osobowych), a także zapewnienie zrównoważonego podejścia, w którym brane będą pod uwagę różne kategorie profilowania oraz różne zagrożenia dla praw osób.

Podczas 91 posiedzenia GR Art. 29 (5-6.06.2013 r.) przyjęta została Opinia 5/2013 w sprawie inteligentnych granic (smart borders), propozycja dotyczące systemu

[406] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

wjazdu/wyjazdu (Entry Exit-System – EES) oraz programu rejestrowania podróżnych (Registered Traveller Programme – RTP) wjeżdżających do strefy Schengen, które zostały przedstawione przez Komisję 28 lutego 2013 r. Przedmiotowa opinia koncentrowała się w szczególności na poważnych obawach odnoszących się do proponowanego systemu EES. Przewiduje on powstanie scentralizowanego systemu służącego do przechowywania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich, którym zezwolono na krótkoterminowy pobyt w strefie Schengen (niezależnie od tego, czy wymagane jest od nich posiadanie wizy Schengen czy też nie). Dane dotyczące tożsamości odwiedzającego oraz długości i celu jego pobytu, będą wprowadzane do systemu przy wjeździe i sprawdzane przy wyjeździe, w celu upewnienia się, że obywatel państwa trzeciego nie przekroczył maksymalnego dopuszczalnego okresu pobytu. Ale scentralizowany system oznacza, że dane mogą być też sprawdzane niezależnie od tego, gdzie obywatel państwa trzeciego wyjeżdża ze strefy Schengen. W opinii członków GR Art. 29 projektowany system wjazdu/wyjazdu przyczyni się do stworzenia nowej bardzo dużej bazy danych i w związku z tym musi spełnić warunek bycia „niezbędnym w demokratycznym społeczeństwie" w celu uzasadnienia swojego wpływu na prawo do ochrony danych osobowych, jak zostało to określone w artykule 8 Karty Praw Podstawowych UE.

Przedmiotem uwagi GR Art. 29 była również kwestia związana z ponownym wykorzystaniem informacji sektora publicznego w Unii Europejskiej. W Opinii 6/2013 (WP 207) dotyczącej przyjętej w dniu 26 czerwca 2013 r. dyrektywy w sprawie ponownego wykorzystywania informacji sektora publicznego (dyrektywy ISP), znalazły się wytyczne dotyczące jej wdrożenia. W dokumencie tym Grupa Robocza Art. 29 podkreśliła, że musi istnieć podstawa prawna do publicznego udostępniania danych osobowych, uwzględniająca podstawowe zasady ochrony danych, jak zasada proporcjonalności, ograniczenia celu oraz minimalizacji zakresu danych. W celu zapewnienia odpowiednich zabezpieczeń zaleca się przeprowadzenie oceny wpływu na ochronę danych, zanim informacje sektora publicznego zostaną udostępnione do ponownego wykorzystania. Ważne jest również, aby warunki wspomnianego zezwolenia obejmowały klauzulę dotyczącą ochrony danych oraz zawierały wytyczne dotyczące jej treści.

Generalny Inspektor Ochrony Danych Osobowych, podczas 92 spotkania europejskich organów zrzeszonych w GR Art. 29 (2-3.10.2013 r.), debatował na temat formuły zgody podmiotu danych na wykorzystywanie plików cookie. Jej rezultatem był „Dokument roboczy

2/2013 przedstawiający wytyczne w sprawie pozyskiwania zgody na zapisywanie plików cookie", w którym – wraz z opinią Grupy w sprawie zgody z 2011 r. oraz opinią z 2012 r. w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody - przedstawione zostały wytyczne dotyczące wymogów ważnej zgody oraz jej głównych elementów w określonym kontekście plików cookie:

1) **Konkretne informacje** - aby zgoda była ważna, musi być konkretna i oparta na odpowiednich informacjach. Ogólna zgoda bez określenia dokładnego celu przetwarzania jest niedopuszczalna.

2) **Termin** - zgoda musi być wyrażona przed rozpoczęciem przetwarzania.

3) **Czynny wybór** - procedura uzyskiwania i wyrażania zgody nie może zastawiać wątpliwości co do zamiaru osoby, której dane dotyczą.

4) **Dobrowolność** - zgoda jest ważna tylko wtedy, gdy podmiot danych ma możliwość dokonania rzeczywistego wyboru.

Ponadto Grupa wysłała pismo do Komisji LIBE (Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego), w którym wyraziła swoje obawy, co do wniosku odnoszącego się do decyzji Rady w sprawie zawarcia porozumienia w zakresie danych dotyczących przelotu pasażera (Passenger Name Record - PNR) między Unią Europejską a Kanadą. Zwrócono przede wszystkim uwagę, że dane te są najczęściej generowane w celach komercyjnych i brak jest rzeczywistych dowodów wskazujących, że wykorzystywanie danych PNR przyczynia się do zwiększenia bezpieczeństwa publicznego.

Ważnym punktem debaty była również kwestia PRISM oraz innych podobnych programów, i jakie mogą być tego konsekwencje dla ochrony prywatności i danych osobowych obywateli Unii Europejskiej.

W tym miejscu podkreślenia wymaga, że w związku z unijnymi pracami nad nowymi ramami prawnymi w zakresie przeciwdziałania praniu pieniędzy i terroryzmowi, europejscy rzecznicy ochrony danych zrzeszonych w GR Art. 29 przygotowali pismo do Sekretariatu Rady, Parlamentu Europejskiego, Komisji Europejskiej oraz Komitetu LIBE, dotyczące nowej dyrektywy w sprawie przeciwdziałania praniu pieniędzy i terroryzmowi (tzw. dyrektywy AML/CFT). W procedurze pisemnego głosowania Generalny Inspektor Ochrony Danych Osobowych opowiedział się za przyjęciem tego pisma.

Natomiast podczas ostatniego, 93 posiedzenia GR Art. 29, w dniu 4 grudnia 2013 r. zostało wydane oświadczenie prasowe, w którym wzywa się wszystkie zainteresowane strony do zintensyfikowania wysiłków w celu przyjęcia pakietu reform ochrony danych osobowych przed końcem obecnej kadencji organów Unii, zaangażowanych w proces legislacyjny. GR Art. 29 uznała głosowanie nad ogólnym rozporządzeniem dotyczącym ochrony danych i dyrektywą dla sektora organów ścigania, które odbyło się w Komisji LIBE w dniu 21 października 2013 r., za znaczący krok w procesie przyjęcia kompleksowych ram prawnych ochrony danych osobowych w Unii Europejskiej. W opinii Grupy, w celu wspierania zaufania obywateli i biznesu do ekonomii cyfrowej, terminowe przyjęcie nowych ram prawnych ochrony danych osobowych, ma bowiem zasadnicze znaczenie dla realizacji jednolitego rynku cyfrowego do 2015 roku.

Generalny Inspektor Ochrony Danych Osobowych, jako przedstawiciel Grupy Roboczej Art. 29, uczestniczył 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 w dniach 30-31 marca 2013 r. Było to już trzecie spotkanie tego Forum z udziałem polskiego organu ds. ochrony danych osobowych. Forum zostało utworzone przez Komisję Europejską. Jest to platforma do wymiany doświadczeń i najlepszych praktyk, które mogą utorować drogę do przyjęcia na szeroką skalę e-fakturowania na poziomie zarówno krajowym, jak i unijnym. Zadaniem Forum jest monitorowanie wprowadzania e-faktur we wszystkich państwach członkowskich. Ma również pomóc Komisji w określeniu dalszych środków ułatwiających przyjęcie systemu e-fakturowania.

W analizowanym 2013 r. GIODO oraz jego przedstawiciele brali również aktywny udział w pracach różnych podgrup powstałych w ramach Grupy Roboczej Art. 29 - Podgrupy ds. Międzynarodowych Transferów Danych, ds. Technologii, ds. Kluczowych Postanowień Dyrektywy, ds. E-administracji i Biometrii, ds. Przyszłości Prywatności oraz Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE). 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 w odniesieniu do prac w ramach Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) GR Art. 29, przedstawiciel GIODO opracował projekt opinii w sprawie zaawansowanych informacji o pasażerach (tzw. danych API).

W 2013 r. przedstawiciel GIODO uczestniczył także w posiedzeniach Podgrupy ds. Technologii. Podczas jednego z takich spotkań, które odbyło się w dniu 25 marca 2013 r. w Brukseli zaplanowane zostało spotkanie z przedstawicielami krajowych regulatorów telekomunikacyjnych, właściwych ds. wdrożenia dyrektywy o prywatności i łączności elektronicznej.

Podczas prac zarówno prac GR Art. 29, jak i Podgrupy ds. Technologii, Podgrupy ds. Biometrii czy eGovernment, GIODO i jego przedstawiciele zgłaszali wiele uwag merytorycznych i redakcyjnych do przygotowywanych podczas posiedzeń dokumentów, a także udzielali informacji w ramach różnego rodzaju ankiet i kwestionariuszy. Wśród nich wymienić należy:

- kwestionariusz w sprawie profilowania dla krajowych organów ochrony danych, w związku z realizacją projektu PROFILOWANIE finansowanego przez Komisję Europejską, DG ds. Sprawiedliwości, w ramach programu Prawa Podstawowe i Obywatelstwo. Projekt skoncentrowany jest na określeniu i zajęciu się wyzwaniami, jakie technologia profilowania stawia podstawowemu prawu do ochrony danych[407].
- kwestionariusz KE w sprawie kompetencji organów krajowych w zakresie informowania podmiotów danych o programach i informacjach tekstowych zapisywanych na ich urządzeniach końcowych oraz realizacji zgłaszania naruszeń ochrony danych wynikających z art. 4(3) oraz 5(3) dyrektywy o E-Prywatności;
- kwestionariusz w zakresie wykorzystywania technologii biometrycznych oraz warunków jakie muszą być spełnione w przypadku jej stosowania. Kwestionariusz przygotowany został przez Podgrupę Grupy Art. 29 ds. Biometrii i e-Government (Biometrics and e-Government Subgroup**);**
- kwestionariusz dotyczący zagadnień związanych z prywatnością i ochroną danych osobowych w odniesieniu do korzystania ze zdalnie sterowanych systemów lotniczych (RPAS) do monitorowania określonej przestrzeni przez użytkowników rządowych, komercyjnych i prywatnych, przesłany do GR Art. 29 przez Komisję Europejską,

[407] Szczegółowe informacje dostępne są na stronach: http://www.unicri.it/special_topics/citizen_profiling/ oraz http://profiling-project.eu/ .

(Questionnaire on privacy and data protection issues related to the utilisation of remotely piloted aircraft systems by governmental, commercial and private users);

- kwestionariusz w sprawie rodzajów usług świadczonych drogą elektroniczną i sposobu ich zabezpieczania, przygotowany przez Podgrupę Grupy Art. 29 ds. E-Government (Questionnaire on data security in e- communication with public sector services) w związku ze zleconymi jej przez Komisję Europejską badaniami nad bezpieczeństwem usług e-Government;
- kwestionariusz przygotowany przez Podgrupę Grupy Art. 29 ds. Nowych Technologii w zakresie dotyczącym oceny skali naruszeń ochrony danych osobowych. W ramach ww. kwestionariusza przygotowano i opracowano ocenę skali przedstawionych przypadków naruszenia ochrony danych wg dwóch wskazanych w kwestionariuszu metod;
- kwestionariusz Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) w sprawie doświadczeń państw członkowskich w kwestii „konieczności" (necessity);
- kwestionariusz oceny stanu wdrożenia do prawa narodowego zaleceń znowelizowanej dyrektywy 2002/58 o E-Prywatności w zakresie dotyczącym informowania użytkowników o programach i innych danych zapisywanych na ich urządzeniach końcowych oraz realizacji zgłaszania naruszeń ochrony danych wynikających z art. 4(3) oraz 5(3) dyrektywy o E-Prywatności;
- Kwestionariusz GR Art. 29 dotyczący praktyk w zakresie inspekcji/egzekwowania prawa.

Na uwagę zasługuje również udział przedstawiciela Generalnego Inspektora Ochrony Danych Osobowych w szkoleniu w zakresie wiążących reguł korporacyjnych (BCR), zorganizowanym w dniach 14-15 listopada 2013 r. w Bonn przez Federalnego Rzecznika Ochrony Danych i Prywatności Niemiec (Training Event 2013). Szkolenie poświęcone było m.in. takim kwestiom jak BCR dla administratorów oraz BCR dla przetwarzających.

Dyskusja nad przygotowanym przez Europejskiego Inspektora Ochrony Danych (European Data Protection Supervisor - EDPS) projektem opinii Grupy Roboczej Art. 29 w sprawie otwartych zasobów i ponownego wykorzystania informacji sektora publicznego (dyrektywa ISP) była głównym tematem spotkania **podgrupy ds. eGovernment, które odbyło się w dniu 3 kwietnia 2013 r.** w Brukseli. Sprawozdawcy projektu przedmiotowej opinii z EDPS podkreślali, że obecny zaawansowany etap prac nad zmianą dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie

ponownego wykorzystania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003 r. s. 90) uniemożliwia dokonywanie w niej istotnych zmian, w szczególności w zakresie ochrony danych osobowych. Przedmiotowe zagadnienie zostało w niej uregulowane w sposób bardzo ogólny i niejednoznaczny (motyw 21, art. 1 ust. 4 dyrektywy ISP), co w konsekwencji doprowadziło do rozbieżności pomiędzy unormowaniami poszczególnych państw członkowskich[408]. Przedstawiciel EDPS zwrócił uwagę na potrzebę bardzo wyraźnego rozróżnienia danych poddanych pseudonimizacji od danych zanonimizowanych. Pseudonimizacja zmniejsza co prawda ryzyko identyfikacji osoby, jednak w większości przypadków dane, wobec których ją zastosowano, będą nadal danymi osobowymi. A zatem decydując o sposobie postępowania z nimi, należy wykazać się znacznie wyższym stopniem skrupulatności, przeprowadzić odpowiednie testy (np. *motivated intruder test)* i ewentualnie przedsięwziąć dodatkowe środki (np. ograniczony dostęp w przypadku danych pochodzących z „wrażliwego" materiału źródłowego lub znacznego ryzyka identyfikacji). Wniosek Komisji dotyczący dyrektywy zmieniającej dyrektywę 2003/98/WE (COM(2011) 877 wersja ostateczna) stwierdza, że dyrektywa nie będzie miała zastosowania do dokumentów nieobjętych prawem dostępu z uwagi na reżimy prawne poszczególnych państw członkowskich w zakresie dostępu do dokumentów. Niemniej jednak zakres tego wyjątku został dokładnie przeanalizowany i można przypuszczać, że ostateczna wersja projektowanych zmian dyrektywy ISP będzie jednak zawierała dodatkowe odniesienia do kwestii danych osobowych, wskazując trzy przypadki, w których dyrektywa ta nie będzie miała zastosowania. Po pierwsze, jeżeli na mocy przepisów prawa krajowego dostęp do dokumentów jest zabroniony. Pamiętać przy tym należy, że nawet jeśli pewne dane osobowe pozostają poza zakresem dyrektywy ISP, nie wyklucza to sytuacji, że dane te mogą być ponownie wykorzystane dla jakiegokolwiek innego celu w innych okolicznościach. W pewnych przypadkach może bowiem istnieć możliwość ponownego wykorzystania danych osobowych, którymi dysponuje sektor publiczny dla innych celów, poddanych dodatkowym zabezpieczeniom oraz podlegających przepisom o ochronie danych osobowych. Po drugie, dyrektywa ISP nie będzie miała zastosowania wobec dokumentów, do których dostęp jest ograniczony na mocy obowiązujących przepisów krajowych w zakresie dostępu, z uwagi na ochronę danych osobowych. Dotyczy to pewnych rodzajów informacji znajdujących się

[408] Uwaga na tę kwestię została zwrócona w dokumencie przygotowanym przez Europejską Sieć Tematyczną LAPSI pt. „Policy Recommendations on Privacy".

w publicznych rejestrach, aktach sądowych bądź dokumentach administracyjnych, które mogą być ujawnione jedynie osobom fizycznym lub organizacjom po wykazaniu interesu prawnego. I trzeci przykład, w którym dyrektywa ISP będzie wyłączona, dotyczy dokumentów lub ich części podlegających udostępnieniu na mocy obowiązujących przepisów prawa krajowego (w zakresie dostępu), które zawierają dane osobowe i których ponowne wykorzystanie zostało określone w przepisach jako niezgodne z prawem dotyczącym ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Okoliczność, że na gruncie prawa krajowego brak jest przepisów, które ograniczałyby ponowne wykorzystanie danych i określałyby cele uzasadniające takie działanie, nie powinna oznaczać, że publicznie dostępne dane osobowe będą każdorazowo dostępne do ponownego korzystania. W takich przypadkach zastosowanie powinny znaleźć ogólne przepisy o ochronie danych osobowych, umożliwiając ocenę, czy dane te powinny zostać udostępnione do ponownego wykorzystania, i jeśli tak, to jakim zabezpieczeniom powinny być poddane. Zasada ponownego wykorzystywania danych nie powinna być bowiem stosowana automatycznie i uchybiać odpowiednim przepisom o ochronie danych osobowych.

Podczas ww. spotkania **podgrupy ds. eGovernment** dyskutowane były również przykłady rozwiązań stosowanych w poszczególnych państwach członkowskich w kwestii sposobu elektronicznej komunikacji obywatela z instytucjami publicznymi. EDPS podniósł, że aktualnie na szczeblu europejskim nie istnieją jednolite ramy prawne w tym zakresie, natomiast podejmuje się szereg inicjatyw na poziomie krajowym. Ale jeśli w wyniku porównania rozwiązań krajowych udałoby się ustalić podobieństwa, to możliwe byłoby w przyszłości opracowanie harmonijnego podejścia w formie rekomendacji w sprawie sposobów komunikowania się obywatela z instytucjami państwowymi. Zagadnienie to będzie więc tematem kolejnych posiedzeń podgrupy.

Z kolei spotkanie zorganizowane przez EDPS 10 kwietnia 2013 r. w Brukseli poświęcone było pakietowi legislacyjnemu dotyczącemu **inteligentnych granic (Smart Borders)**. Pakiet ten składa się z trzech projektów rozporządzeń dotyczących programu rejestrowania podróżnych (Registered Traveller Programme – RTP), systemu wjazdu/wyjazdu (Entry Exit System - EES) oraz zmieniającego Kodeks Graniczny Schengen. Podczas tego spotkania dyskutowane były wątpliwości, jakie budzą kwestie niezbędności oraz proporcjonalności proponowanych systemów, jak również dostęp organów ścigania do przechowywanych w nich danych.

Natomiast w dniach 11-12 kwietnia 2013 r. w Brukseli odbyły się posiedzenia grup koordynujących nadzór nad **VIS i Eurodac (CSG VIS i Eurodac)**, którym przewodniczył Peter Hustinx, Europejski Rzecznik Ochrony Danych Osobowych. Podczas tych spotkań poruszono tematy krajowych inspekcji i doświadczeń z wdrażania obu systemów, zaś Komisja Europejska oraz Agencja Unii Europejskiej ds. zarządzania wielkoskalowymi systemami IT (European Agency for the operational management of large-scale IT systems - EU-LISA), przedstawiły informacje z postępów wdrażania VIS na poziomie centralnym oraz informację o stanie prac nad zmianą rozporządzenia o Eurodac, ze szczególnym uwzględnieniem kwestii dostępu organów ścigania do tego systemu. Debatowano także nad treścią dokumentów dotyczących przyszłego programu prac obu grup.

W analizowanym 2013 r. przedstawiciel GIODO uczestniczył również w posiedzeniach **Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupy Berlińskiej)**, z których jedno odbyło się w dniach 15-16 kwietnia 2013 r. w Pradze, drugie zaś 2-3 września 2013 r. w Berlinie. Na spotkaniach tych przedstawiany był krajowy raport dotyczący ochrony prywatności i danych osobowych w usługach telekomunikacyjnych, z uwzględnieniem zmian w polskim prawie, które odnoszą się do zagadnień związanych z ochroną danych osobowych, a także charakterystyka działań na tym polu zarówno GIODO, jak i innych zainteresowanych podmiotów.

Natomiast 18 września 2013 r. w Brukseli, przedstawiciel GIODO – członek Zespołu do Spraw Naruszeń Danych Osobowych – był uczestnikiem spotkania zorganizowanego przez Komisję Europejską nt. technicznych środków implementacyjnych przyjętych 24 czerwca 2013 r. W spotkaniu tym udział wzięli przedstawiciele wszystkich właściwych organów krajowych odpowiedzialnych za zgłoszenia naruszeń ochrony danych osobowych na mocy dyrektywy o prywatności i łączności elektronicznej.

Omawiając zagadnienie współpracy międzynarodowej GIODO podkreślenia wymagają również działania - zasygnalizowane w innej części *Sprawozdania* - podejmowane przez niego w ramach **projektu PHAEDRA** w zakresie wspierania współpracy między organami ochrony danych. Gwałtowny rozwój technologii informacyjno-komunikacyjnych doprowadził do wzrostu transgranicznego przekazywania danych osobowych oraz zwiększenia zagrożeń ochrony danych i prywatności. Poradzenie sobie z naruszeniami ochrony danych i prawa do prywatności wymaga więc odpowiednich działań i współpracy miedzy podmiotami działającymi w tym obszarze. I tak, w 2007 r. OECD przyjęło Rekomendację w sprawie

transgranicznej współpracy w sprawie stosowania przepisów dotyczących ochrony prywatności, podczas 29. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności (Montreal, 2007 r.) uchwalono „Rezolucję w sprawie współpracy międzynarodowej", w 2010 r. 11 organów odpowiedzialnych za egzekwowanie przepisów regulujących ochronę prywatności, utworzyło Światową Sieć Egzekwowania Przepisów o Ochronie Prywatności (Global Privacy Enforcement Network – GPEN), której misją jest propagowanie i wspieranie współpracy transgranicznej w zakresie egzekwowania przepisów dotyczących ochrony prywatności, głównie poprzez wymianę informacji między organami ochrony danych, natomiast podczas 33. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności (Mexico City, 2011 r.) przyjęto nawet bardziej szczegółową rezolucję zachęcającą do intensyfikacji działań na rzecz skutecznej koordynacji transgranicznych dochodzeń i egzekwowania prawa. Jak widać na przedstawionych przykładach, potrzebę wzmocnienia współpracy w obszarze egzekwowania prawa do prywatności i ochrony danych dostrzeżono już na początku XXI wieku. Ale mimo podjęcia określonych wysiłków, kwestia ta nadal pozostaje jednym z najsłabszych ogniw w zarządzaniu ochroną danych i prywatności Projekt PHAEDRA jest więc kolejną międzynarodową inicjatywą mającą na celu usprawnienie współpracy i koordynacji działań między organami ochrony danych osobowych. *„Codziennie toczy się bitwa o każdego obywatela. Rządy, przedsiębiorcy, hakerzy i inni wyrządzający krzywdy, próbują odrzeć obywateli z prywatności. Naszymi głównymi, słabo uzbrojonymi obrońcami są organy ochrony danych i rzecznicy ochrony prywatności"* – powiedział David Wright, partner zarządzający Trilateral Research & Consulting (Zjednoczone Królestwo) projektu PHAEDRA, w oświadczeniu prasowym z dnia 20 lutego 2013 r.[409] Natomiast w opinii GIODO, jednego z czterech partnerów tego projektu, z uwagi na ogólnoświatowy zasięg tych zagrożeń, należy zrobić krok dalej. Konieczna jest tu zdecydowana globalna odpowiedź na zagrożenia, w postaci działań skupiających się nie tylko na ochronie danych osobowych i prywatności obywateli europejskich, ale również na współpracy z krajami spoza UE w celu zapewnienia egzekwowania przepisów dotyczących ochrony danych wobec międzynarodowych administratorów danych i innych, którzy naruszają prawa w tym zakresie.

[409] www.giodo.gov.pl/plik/id_p/4211/j/pl/

Podkreślenia wymaga, że również w programie Grupy Roboczej Art. 29 znajduje się kwestia wzmocnienia wysiłków na rzecz skoordynowanych i spójnych działań w zakresie egzekwowania prawa, w celu zapewnienia większej zgodności w całej Unii Europejskiej. Akcentując jedynie kontekst europejski, GR Art. 29 zwróciła także uwagę, że wiele organów ochrony danych spotyka się z ograniczeniami prawnymi, instytucjonalnymi oraz z niedoborem zasobów ludzkich i finansowych. Dlatego wskazała m.in. na konieczność opracowania zasad wzajemnej współpracy między nimi w taki sposób, aby zwiększyć ich skuteczność oraz obniżyć koszty ich działalności poprzez m.in. wyeliminowanie zjawiska dublowania zadań.

W odniesieniu do współpracy międzynarodowej podkreślić należy także aktywny udział Generalnego Inspektora Ochrony Danych Osobowych i jego przedstawicieli w spotkaniach organizowanych przez Europejską Agencję Bezpieczeństwa Informacji i Sieci (ENISA).

Oprócz przedstawionych powyżej przykładów 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 Praty on Information Exchange and Data Protection – DAPIX), w której aktywnie uczestniczył Generalny Inspektor Ochrony Danych Osobowych, udzielając polskiej delegacji merytorycznego wsparcia. Współpraca między Senatem RP a Generalnym Inspektorem Ochrony Danych Osobowych (w tym wspólne posiedzenie Komisji Praw Człowieka, Praworządności i Petycji oraz Komisji Spraw Unii Europejskiej w dniu 16 kwietnia 2013), polegała na udzielaniu informacji, w szczególności w zakresie przebiegu prac nad reformą prawa o ochronie danych osobowych w UE.

I tak, w dniach 23-24 września 2013 r. miała miejsce wizyta studyjna w Brukseli z udziałem delegacji Senatu RP, w skład której weszli członkowie Komisji Spraw Unii Europejskiej oraz przewodniczący komisji branżowych. Program tego spotkania przewidywał spotkanie z przedstawicielami Komisji ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego, w celu omówienia zagadnień związanych z ochroną danych osobowych. Wzorem poprzednich lat, Generalny Inspektor Ochrony Danych Osobowych przygotował na to spotkanie informację oraz tezy do rozmów na podany temat.

W podsumowaniu podkreślenia wymaga, że w ramach współpracy na forum międzynarodowym Generalny Inspektor Ochrony Danych Osobowych w 2013 r. przekazywał regularnie swoje uwagi do stanowisk Rządu RP oraz do instrukcji na posiedzenia gremiów przygotowawczych Rady Unii Europejskiej w odniesieniu do następujących projektów aktów prawnych Unii Europejskiej:

- projektu dyrektywy w sprawie ochrony danych osobowych przetwarzanych do celów zapobiegania i zwalczania przestępczości, wykrywania i ścigania ich sprawców albo wykonywania orzeczeń sądowych w sprawach karnych, w ramach Grupy Roboczej Rady UE ds. wymiany informacji i ochrony danych osobowych (Working Party on Information Exchange and Data Protection - DAPIX);
- projektu rozporządzenia w sprawie Agencji Unii Europejskiej ds. Współpracy i Szkolenia w Dziedzinie Egzekwowania Prawa (Europol) w ramach prac Grupy Roboczej ds. egzekwowania prawa (Law Enforcement Working Party - LEWP) oraz Komitetu Koordynacyjnego ds. współpracy policyjnej i sądowej w sprawach karnych (Coordinating Committee in the area of police and judicial cooperation in criminal matters - CATS*);*
- projektu pakietu legislacyjnego dotyczącego Inteligentnych Granic (*Smart Borders)* w ramach grupy roboczej ds. granic (Frontiers Working Party).

Na podkreślenie zasługuje także aktywny udział GIODO – jako eksperta krajowego – w wydarzeniu zorganizowanym przez Dyrekcję ds. Rozszerzenia Komisji Europejskiej w ramach TAIEX (Technical Assistance and Information Office), podczas którego przedstawiał prezentacje tematyczne. I tak, w dniach 29-30 maja 2013 r. w Skopje w Macedonii brał udział w seminarium dotyczącym społecznej i prawnej odpowiedzialności za łamanie prawa o ochronie danych osobowych. Natomiast przedstawiciel polskiego organu

ds. ochrony danych osobowych uczestniczył w charakterze eksperta krajowego w misji Komisji Europejskiej w ramach prowadzonego przez nią dialogu wizowego z Rosją (Moskwa, 7-12.04.2013 r.)

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, cloud computing, działania podejmowane przez polski organ ds. ochrony danych osobowych w świetle rewizji unijnych ram prawnych ochrony danych, wykorzystywanie bazy ADAMS przez polską organizację antydopingową, procedura zgłaszania zbiorów danych do rejestracji GIODO, itp.

Nadawcami pytań były też inne organizacje i instytucje, działające na polu ochrony praw podstawowych. Na uwagę zasługuje prośba Węgierskiej Unii Praw Obywatelskich o przekazanie przez GIODO informacji na potrzeby projektu badawczego dotyczącego ochrony danych. Węgierska instytucja prosiła o informacje na temat baz danych prowadzonych przez różne organizacje i instytucje, w szczególności przez Policję, sądy, służbę zdrowia i oświatę, w celu oceny zagrożeń i zebrania informacji o najlepszych praktykach podejmowanych w tej dziedzinie.

9.1. 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 2013 roku, współorganizowanym przez GIODO, były - opisane w innej części niniejszego Sprawozdania - uroczystości związane z obchodami **VII Europejskiego Dnia Ochrony Danych Osobowych, które odbywały się w Brukseli w dniach 22-23 stycznia 2013 r.** W trakcie obchodów tego święta Generalny Inspektor Ochrony Danych Osobowych wziął udział w sesji

polskiej podczas 6. Międzynarodowej Konferencji pt. „Computers, Privacy and Data Protection (CPDP) 2013. Reloading Data Protection", podczas której omawiane były tematy dotyczące dostępu władz publicznych do informacji o obywatelach, projekt INDECT oraz przetwarzanie danych osobowych przez kościoły i związki wyznaniowe. Brał również udział w uroczystym spotkaniu ekspertów ochrony danych osobowych z posłami do Parlamentu Europejskiego, przedstawicielami Rady Europy, Komisji Europejskiej, polskich ministerstw, urzędów centralnych i placówek dyplomatycznych w Brukseli oraz innych polskich i unijnych instytucji.

Postępująca globalizacja i stopień komplikacji kwestii związanych z wykorzystywaniem danych osobowych powodują, że rzecznicy ochrony danych osobowych z kilkudziesięciu krajów świata spotykają się regularnie, by wspólnie dyskutować o najważniejszych problemach w dziedzinie ochrony prywatności i danych osobowych oraz szukać możliwych rozwiązań. **35. Międzynarodowa Konferencja Rzeczników Ochrony Danych**, której gospodarzem był Generalny Inspektora Ochrony Danych Osobowych (Warszawa, 23-26.09.2013 r.), była okazją do dyskusji, jak w zglobalizowanym świecie, w którym funkcjonują różne porządki prawne, skutecznie chronić dane osobowe i prywatność. Hasło przewodnie 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności *Prywatność: przewodnik po zagmatwanym świecie,* to reakcja na problemy współczesnego świata, w którym coraz bardziej skomplikowane metody przetwarzania informacji oraz zawiłe relacje łączące poszczególne podmioty, rzutują na bezpieczeństwo danych. Za przykład może posłużyć wykorzystywanie danych osobowych przez międzynarodowe korporacje, przetwarzanie danych w chmurze obliczeniowej, czy korzystanie z portali internetowych, nierzadko mających swoje serwery w różnych państwach i często niespełniających unijnych standardów w zakresie bezpieczeństwa danych. Światowa konferencja rzeczników ochrony danych i prywatności zgromadziła 66 delegacji rzeczników z 52 krajów - nie tylko państw Unii Europejskiej, lecz również z Australii, Stanów Zjednoczonych Ameryki, Meksyku, Nowej Zelandii, Mauritiusa, Burkina Faso, Urugwaju, Kanady i in. Spotkanie w takim gronie umożliwiło zderzenie różnych spojrzeń na kwestie prywatności i ochrony danych osobowych, wypracowanie spójnego podejścia do zagadnień, które mają charakter globalny, przy jednoczesnym zwróceniu uwagi na te problemy, które pojawiły się już w konkretnych państwach, a w innych jeszcze nie są odczuwane. Podczas tego najważniejszego corocznego spotkania rzeczników ochrony danych i prywatności z całego świata, uczestnicy dyskutowali

o wielu szczegółowych kwestiach w perspektywie różnic kulturowych i doświadczeń poszczególnych krajów, odmiennych systemów prawnych oraz rozwiązań technicznych i technologicznych obowiązujących w każdym z nich.

Pierwsze dwa dni Konferencji były zamkniętymi spotkaniami rzeczników ochrony danych z całego świata, które zakończyły się przyjęciem 8 rezolucji oraz Deklaracji Warszawskiej w sprawie upowszechniania się aplikacji w społeczeństwie. Dokumenty te zawierają wskazania dla rzeczników, które powinny być brane pod uwagę zarówno przy wydawaniu decyzji w konkretnych sprawach, jak i przy opiniowaniu aktów prawnych.

1) **Rezolucja dotycząca profilowania**, tj. pozyskiwania z różnych źródeł informacji o osobach, następnie zestawiania ich i wyciągania na tej podstawie kolejnych wniosków w celu stworzenia profilu, była rezultatem debaty przeprowadzonej w czasie 34. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, która odbyła się w Urugwaju. Uczestnicy tegorocznej Konferencji zwrócili uwagę na wiele pożytecznych zastosowań Big Data w polityce, biznesie, czy w działalności organizacji non-profit. Przywołując ogólne zasady ochrony danych i prywatności uznali, że zjawisko profilowania powinno być ograniczone do niezbędnego minimum. Podkreślili również konieczność informowania użytkowników o tym, że podlegają profilowaniu, nawet w przypadku, gdy profilowanie odbywa się w oparciu o powszechnie dostępne źródła.
2) **Rezolucja w sprawie jawności praktyk w zakresie ochrony danych osobowych** zwraca szczególną uwagę na konieczność informowania podmiotu danych – w jasny i przystępny sposób – kto i w jakim celu gromadzi jego dane osobowe, jak można się z nim skontaktować oraz jakie są sposoby żądania dostępu do danych, w celu np. ich poprawienia. W dokumencie tym kładzie się szczególny nacisk na konieczność poinformowania osoby, której dane są gromadzone, o obowiązującej w danym podmiocie polityce prywatności.
3) **Rezolucja w sprawie śledzenia w sieci i ochrony prywatności** dotyczy coraz powszechniejszego zjawiska śledzenia zachowań użytkowników sieci (web tracking). Rzecznicy zwracają w niej uwagę , że tego typu monitoring zagraża prywatności i stwarza możliwość budowania profili internautów. Zaapelowali więc, by wszyscy interesariusze, w tym rządy, organizacje międzynarodowe oraz dostawcy usług zapewnili, że ochrona prywatności będzie przez nich traktowana priorytetowo podczas projektowania i wykonywania usług społeczeństwa informacyjnego w przyszłości.

4) **Rezolucja w sprawie edukacji cyfrowej dla wszystkich** podkreśla konieczność zapewnienia konsumentom i przedsiębiorcom dostępu do wiedzy dotyczącej cyfrowej technologii, by stali się aktywnymi, kreatywnymi oraz świadomymi jej użytkownikami.
5) **Rezolucja na rzecz zapewnienia ochronie danych osobowych i prywatności stałego miejsca w prawie międzynarodowym** wskazuje na pilną potrzebę stworzenia wiążącego międzynarodowego porozumienia w sprawie ochrony danych, które zabezpieczy prawa człowieka, ochronę prywatności, danych osobowych i integralność sieci, a także zwiększy przejrzystość przetwarzania danych, przy zachowaniu równowagi między poszanowaniem bezpieczeństwa a interesami gospodarczymi. Rezolucja zakłada dążenie do stworzenia standardów prawnych w zakresie ochrony danych osobowych o globalnym zasięgu.
6) **Rezolucja w sprawie koordynacji międzynarodowego egzekwowania prawa** kładzie nacisk na konieczność wzmocnienia współpracy i koordynacji działań na rzecz egzekwowania prawa o ochronie danych i prywatności w skali międzynarodowej.
7) **Rezolucja w sprawie strategicznego kierunku Konferencji** koncentrowała się na określeniu kierunków rozwoju oraz misji corocznych Międzynarodowych Konferencji Rzeczników Ochrony Danych i Prywatności, w szczególności w odniesieniu do zadań, które będą przyświecały grupom roboczym przez najbliższy rok, do następnego Spotkania.
8) **Rezolucja w sprawie akredytacji.** Podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności przyznano akredytacje członkowskie rzecznikom ochrony danych z Mauritiusu, Kosowa oraz Buenos Aires z Argentyny, zaś akredytacje obserwatora reprezentantom Południowej Korei, Rosji, Kanady, Singapuru, Bremy oraz dwóm urzędom z Ekwadoru.

Podsumowaniem dyskusji pierwszego dnia obrad była **Deklaracja Warszawska sprawie upowszechniania się aplikacji w społeczeństwie.** Rzecznicy zwracają w niej uwagę, że wprawdzie aplikacje ułatwiają codzienne życie, a także zapewniają rozrywkę, lecz równocześnie umożliwiają przetwarzanie dużej ilości danych, często bez wiedzy osób, których one dotyczą. Kluczowe jest więc, aby ich użytkownicy posiadali kontrolę nad swoimi danymi, a przetwarzanie odbywało się zgodnie z prawem. Chociaż w pierwszym rzędzie za odpowiednią ochronę prywatności odpowiedzialne są spółki zajmujące się aplikacjami, nie tylko ich twórcy oraz dostarczyciele systemów operacyjnych, ale także organy publiczne regulujące ten sektor powinny podnosić świadomość w tym zakresie – i to zarówno wśród podmiotów oferujących aplikacje, jak i w całym społeczeństwie.

Zakończeniem dwudniowych obrad zamkniętych były **pierwsze warsztaty projektu PHAEDRA (24.09.2013 r.) skierowanego na poprawę współpracy i koordynacji miedzy organami ochrony danych**, z udziałem ponad 70 przedstawicieli organów ochrony danych, rzeczników ds. ochrony prywatności, organów ds. egzekwowania ochrony danych i prywatności oraz innych zainteresowanych podmiotów[410].

Kolejne dwa dni Konferencji – 25 i 26.09.2013 r. – miały charakter otwarty i przebiegały z udziałem przedstawicieli wielu środowisk ze świata polityki, nauki, biznesu oraz krajowych i międzynarodowych organizacji pozarządowych, którzy debatowali w grupach podzielnych na trzy ścieżki tematyczne: „Reformy na świecie. Interoperacyjność między regionami", „Ochrona prywatności a technologia", „Interesariusze: perspektywy, role, interesy". Uczestnicy pierwszej z nich mieli okazję zapoznać się z planowanymi zmianami prawa dotyczącego ochrony danych osobowych, które przewidują zastąpienie wszystkich 28 ustaw o ochronie danych osobowych, jednym europejskim rozporządzeniem oraz o pracach nad przygotowaniem przepisów dotyczących ochrony prywatności w ramach APEC-organizacji zrzeszającej państwa Azji i Pacyfiku, w skład której wchodzą kraje takie, jak Nowa Zelandia, Australia, USA, Japonia, Chiny i Rosja. Podczas tej ścieżki tematycznej mowa była głównie na temat interoperacyjności regionów – co dzieli i przeszkadza, a co łączy i umożliwia współpracę między regionami. Druga ścieżka tematyczna dotyczyła kwestii technicznych i wpływu nowych technologii na ochronę danych osobowych i prywatności. Zaś trzecia związana była z różnicami w podejściu do ochrony prywatności i danych osobowych, z jakimi mamy do czynienia w poszczególnych państwach, czego przykładem była sprawa PRISM czy amerykańskiej ustawy FATCA, nakazującej instytucjom finansowym współpracującym z USA, przekazywanie informacji o klientach na potrzeby amerykańskiego fiskusa.

W trzecim dniu Konferencji, tj. 25 września 2013 r., Konfederacja Europejskich Organizacji Inspektorów Ochrony Danych (Confederation of European Data Protection Organisations – CEDPO) oraz krajowe stowarzyszenia zrzeszające inspektorów ochrony danych w Europie, w tym Stowarzyszenie Administratorów Bezpieczeństwa Informacji (SABI) w Polsce, przyjęły **Deklarację Warszawską 2013**, **dotyczącą zachęcania**

[410] Więcej informacji na temat projektu można znaleźć na stronie internetowej www.phaedra-project.eu zaś program warsztatów dostępny jest na stronie http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-Workshop-Agenda-20_09_13.pdf .

organizacji w Europie do wyznaczania inspektorów ochrony danych osobowych (Data Protection Officer – DPO)[411]. Podkreślono w niej coraz większą rolę DPO, jako ważnego „przewoźnika" zapewniającego zgodne z zasadami ochrony danych funkcjonowanie danej organizacji w praktyce.

Ponieważ organizacja Konferencji zbiegła się w czasie z przypadającym w 2013 roku 15-leciem obowiązywania ustawy o ochronie danych osobowych, był to również dobry moment, by dokonać oceny tych przepisów. W opinii GIODO, choć główne zasady i przyjęta w ustawie konstrukcja dochodzenia prawa ochrony danych osobowych się sprawdziły, to jednak część polskich przepisów o ochronie danych osobowych nie przystaje do rzeczywistości i wymaga zmian. Spowodowane jest to m.in. postępem technologicznym, zwłaszcza rozwojem Internetu. Postępująca globalizacja wymusza również korektę regulacji dotyczących międzynarodowej wymiany danych. Ponadto, w ocenie GIODO, niektóre rozwiązania, jak np. obowiązek rejestracji zbiorów danych osobowych, były potrzebne na początku obowiązywania ustawy, lecz dziś są zbędne. Rozważenia wymaga też liczba wyjątków od ogólnych zasad ochrony danych osobowych, bowiem niektóre są być może uzasadnione, ale część na pewno wymaga już przeanalizowania.

Z okazji obchodów 15. rocznicy uchwalenia ustawy o ochronie danych osobowych, która przypadła na dzień 29 sierpnia 2013 r., Generalny Inspektor Ochrony Danych Osobowych wydał okolicznościowy Album będący podsumowaniem tego okresu. W publikacji tej znalazły się zarówno referaty, jak i osobiste wspomnienia osób, które pracowały przy tworzeniu ustawy i jej kolejnych nowelizacjach, pisały pierwsze komentarze do ustawy, od początku pracowały w Biurze GIODO lub z nim współpracowały. Zaletą Albumu jest przedstawiona w nim różnorodność spojrzenia na proces tworzenia prawa o ochronie danych osobowych, pierwsze dni działalności Biura z perspektywy 15 lat ustawy, widziane oczami konkretnych osób.

Honorowy patronat nad 35. Międzynarodową Konferencją Rzeczników Ochrony Danych i Prywatności sprawowali: Prezydent Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Ministerstwo Sprawiedliwości i Ministerstwo Spraw Wewnętrznych.

[411] W polskich przepisach zdefiniowany jako Administrator Bezpieczeństwa Informacji.

Wśród innych najważniejszych wydarzeń o charakterze międzynarodowym, które odbyły się z udziałem GIODO lub jego przedstawicieli znalazły się:

1. **6. Międzynarodowa Konferencja „Computers, Privacy and Data Protection (CPDP) 2013. Reloading Data Protection" (Bruksela, 23-25.01.2013 r.)**

W związku z obchodami Europejskiego Dnia Ochrony Danych Osobowych, tradycyjnie od 6 lat odbywa się w Brukseli Międzynarodowa Konferencja „Komputery, Ochrona Danych i Prywatności". W pierwszym dniu Konferencji Generalny Inspektor Ochrony Danych Osobowych zorganizował specjalny panel poświęcony prawu do prywatności i ochrony danych osobowych w Polsce, zatytułowany „From 'Solidarity' to the Surveillance Society. Privacy Protection Dilemmas in Poland" (Od solidarności do społeczeństwa nadzorowanego. Dylematy związane z ochroną danych osobowych w Polsce"). Wydarzenie to zorganizowane było przez Vrije Universiteit Brussel (Research Group on Law, Science, Technology and Society – LSTS), Facultès 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.

2. **Konferencja poświęcona ochronie prywatności online (Malta, 20-21.03.2013 r.)**

W dniach 20-21 marca 2013 r. Generalny Inspektor Ochrony Danych Osobowych, uczestniczył w Konferencji poświęconej ochronie prywatności online zatytułowanej „Online Privacy: Consenting to your Future" zorganizowanej i finansowanej w ramach projektu „CONSENT" 7 Programu Ramowego Unii Europejskiej na Malcie[412]. Konferencja stanowiła podsumowanie prac nad projektem „CONSENT", będącym największym wspieranym przez UE projektem badawczym, którego celem jest zbadanie, w jaki sposób zachowania konsumentów i praktyki handlowe wpływają na zagadnienie zgody przy przetwarzaniu danych osobowych. Rangę temu wydarzeniu nadał udział w nim Europejskiego Inspektora Ochrony Danych Osobowych, Wiceprzewodniczącej Komisji Europejskiej oraz przedstawicieli Parlamentu Europejskiego.

Pierwszego dnia Konferencji podczas sesji pn. „Prawo do bycia zapomnianym", Generalny Inspektor Ochrony Danych Osobowych wygłosił referat zatytułowany „Prawo do bycia zapomnianym. Podstawowe prawo osoby czy niebezpieczeństwo 'Ministerstwa Prawdy'".

[412] http://www.consent.law.muni.cz/view.php?cisloclanku=2010080004.

Z kolei drugiego dnia Konferencji wziął udział w dyskusji panelowej zatytułowanej „Obecna sytuacja jako kontekst dla Opcji Polityki CONSENT. Rola europejskich organów ochrony danych".

3. Seminarium „The Right to be Forgotten" (Cambridge, 09.04.2013 r.)

Seminarium na temat prawnych aspektów „Prawa do bycia zapomnianym", które odbyło się 9 kwietnia 2013 r. na Wydziale Prawa Uniwersytetu w Cambridge, zorganizowane zostało przez Centre for European Legal Studies (CELS). Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych przedstawił prezentację pt. „Right to be forgotten and freedom of expression", w której przedstawił stosunek prawa do bycia zapomnianym w odniesieniu do innych analogicznych praw, w szczególności wolności słowa, kreśląc jego skutki dla społeczeństwa oraz Internetu.

4. XV Spotkanie Rzeczników Ochrony Prywatności z Krajów Europy Środkowej i Wschodniej (Belgrad, 10-12.04.2013 r.)

W dniach 10-12 kwietnia 2013 r. w Belgradzie Generalny Inspektor Ochrony Danych Osobowych wziął udział w 15. Spotkaniu Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA)[413]. Gospodarzem tegorocznego wydarzenia był organ ochrony danych Serbii. Wśród uczestników spotkania znaleźli się przedstawiciele 14 organów ochrony danych z następujących krajów: Albanii, Bośni i Hercegowiny, Bułgarii, Węgier, Republiki Macedonii, Polski, Rosji, Słowacji, Słowenii, Serbii, Ukrainy, Chorwacji, Czarnogóry i Republiki Czeskiej. Obrady skupiły się wokół trzech zagadnień: bezpieczeństwo danych, przetwarzanie danych osobowych w kontekście zatrudnienia oraz niezależność organów ochrony danych, stojących wobec wyzwań związanych z globalizacją i rozwojem nowoczesnych technologii. W czasie pierwszej sesji poświęconej bezpieczeństwu danych zajęto się dwoma tematami. Pierwszy dotyczył nowych kierunków w procesie przetwarzania danych osobowych w sektorze publicznym, w szczególności w sferze przetwarzania elektronicznego oraz oceny wpływu na ochronę prywatności. W ramach drugiego tematu przedstawiono przykłady naruszeń ochrony danych w poszczególnych krajach. Podczas drugiej sesji dotyczącej przetwarzania danych w kontekście zatrudnienia uczestnicy omówili różnorodne metody kontroli pracowników, wpływ technologii informacyjno-

[413] Grupa Państw Europy Środkowej i Wschodniej powołana została z inicjatywy Generalnego Inspektora Ochrony Danych Osobowych w 2001 roku. Polski organ ochrony danych pełni funkcję sekretariatu CEEDPA.

komunikacyjnych na prawa osób, których dane dotyczą, a szczególnie aspekt ochrony prawnie uzasadnionego interesu pracodawcy oraz ochrony prawa do poszanowania godności pracownika. Uczestnicy omówili kwestie przeprowadzania testów wśród kandydatów do pracy w ramach procedur związanych z zatrudnieniem i rekrutacją oraz zgodnie wyrazili pogląd w kwestii zgody na przetwarzanie danych w kontekście zatrudnienia, podkreślając że nie jest to zgoda dobrowolna. Trzecia sesja poświęcona była niezależności organów ochrony danych i wyzwaniom, z jakimi mają do czynienia. Dyskusja na ten temat skoncentrowana była na kwestiach transgranicznego przekazywania danych, monitoringu obszarów publicznych oraz wypowiedzi szerzących nienawiść, zwłaszcza w mediach. Uczestnicy dyskusji podkreślili, że niezależność organów ochrony danych osobowych oznacza, że powinny być one oddzielone organizacyjnie i funkcjonalnie od administracji publicznej i innych organów publicznych, których działania muszą kontrolować. Podczas tego wydarzenia, Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Privacy Impact Assessment for eGovernmental Clouds", w którym przybliżył zagadnienia ochrony prywatności w fazie projektowania usług chmurowych w e-administracji.

W czasie spotkania ustalono również, że kolejne 16. Spotkanie CEEDPA odbędzie się w 2014 r. w Skopje. Ponadto przedstawiciele organów ochrony danych Węgier oraz Bośni i Hercegowiny wyraziły wolę zorganizowania 17. Spotkania CEEDPA w 2015 r., ale decyzja w tej sprawie zostanie podjęta na wspomnianym spotkaniu w Republice Macedonii. Ustalono także, że Federacja Rosyjska, posiadająca dotychczas status obserwatora w Grupie Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, uzyska pełne członkostwo.

5. Międzynarodowa Konferencja „Data Protection Intensive" (Londyn, 24-25.04.2013 r.)

O relacjach pomiędzy nowoczesnymi technologiami a prawem do prywatności i ochrony danych osobowych dyskutowano w trakcie Międzynarodowej Konferencji „Data Protection Intensive" w Londynie. Wskazywano coraz to nowe obszary zastosowań nowoczesnych rozwiązań technologicznych, podkreślając ich użyteczność i wygodę dla obywatela, w szczególności w perspektywie postępującej globalizacji oraz starzenia się społeczeństw. Poszukiwaniu równowagi pomiędzy postępem technologicznych a prawem do prywatności i ochrony danych osobowych, zwłaszcza danych wrażliwych, poświęcone było także wystąpienie Generalnego Inspektora Ochrony Danych Osobowych pt. „Sensitive Data and

Emerging Technologies: Friends or Foes". Organizatorem tego międzynarodowego wydarzenia było IAPP (International Association of Privacy Professionals) zrzeszające praktyków z ponad 80 krajów zajmujących się tematyką ochrony prywatności.

6. Międzynarodowa Konferencja „European Identity & Cloud Conference 2013" (Monachium, 13-17.05.2013 r.)

„Personal Data Protection and eID. Bringing two reforms of EU law to common denominator" – to tytuł wystąpienia Generalnego Inspektora Ochrony Danych Osobowych podczas międzynarodowej konferencji „European Identity & Cloud Conference 2013". Motywem przewodnim tego wydarzenia była kwestia europejskiej tożsamości w kontekście innowacyjnych rozwiązań chmurowych w zarządzaniu bezpieczeństwem informacji. W trakcie obrad dyskutowano nad strategią zgodnego z prawem ochrony danych wdrażania systemów bezpieczeństwa informacji w Cloud computingu oraz jak przygotować sektor biznesu na wejście w życie nowego unijnego prawa o ochronie danych. Organizatorem Konferencji był KuppingerCole.

7. Wiosenna Konferencja Rzeczników Ochrony Danych (Lizbona, 16-17.05.2013 r.)

Generalny Inspektor Ochrony Danych Osobowych oraz Dyrektor Departamentu Edukacji Społecznej Współpracy Międzynarodowej wzięli udział w zorganizowanej przez portugalski organ ochrony danych (CNPD) Wiosennej Konferencji Rzeczników Ochrony Danych pt. „Ochrona prywatności i związane z nią wyzwania". Podczas sesji poświęconej bezpieczeństwu informacji GIODO wygłosił wykład pt. „Co oznacza bezpieczeństwo w świecie w chmurach ".

W trakcie Konferencji Europejscy Rzecznicy Ochrony Danych przyjęli cztery rezolucje:

- Rezolucję w sprawie przyszłości ochrony danych w Europie,
- Rezolucję na rzecz zapewnienia ochrony danych w transatlantyckiej strefie wolnego handlu (współwnioskodawcą był Generalny Inspektor Ochrony Danych Osobowych),
- Rezolucję w sprawie Europolu,
- Rezolucję w sprawie akredytacji (na jej mocy organ ochrony danych Serbii został akredytowany jako członek, zaś organ ochrony danych Republiki Kosowa - jako stały obserwator Konferencji Europejskich Organów Ochrony Danych).

8. IV Międzynarodowa Konferencja „Współpraca Międzynarodowa jako forma zagwarantowania ochrony prywatności w każdym kraju" (Moskwa, 5-8.11.2013)

Głównymi tematami Konferencji była kwestia modernizacji ustawodawstwa europejskiego, w szczególności w kontekście wyzwań i zagrożeń związanych z wdrożeniem IT do codziennego życia, oraz nowe naruszenia prawa i zapobieganie im, w aspekcie świadczeń wzajemnej pomocy. Uczestnikami tego wydarzenia byli przedstawiciele organów ochrony danych z Europy, Regionu Azji i Pacyfiku, rosyjskich organów legislacyjnych i wykonawczych, a także największych firm internetowych oraz członków społeczności eksperckiej. Organizatorem Konferencji był Rosyjski Urząd ds. Ochrony Danych.

9.2. Wizyty robocze

1. Spotkanie GIODO z Dyrektor Generalną ds. Sprawiedliwości KE

W dniu 1 marca 2013 r. Generalny Inspektor Ochrony Danych Osobowych gościł w swoim Biurze Panią Françoise Le Bail, Dyrektor Generalną ds. Sprawiedliwości Komisji Europejskiej. Spotkanie poświęcone było przedstawieniu dotychczasowego stanu prac nad unijną reformą ochrony danych oraz przewidywanym kierunkom jej zmian. W szczególności poruszone zostały kwestie, które w toczącej się debacie wywołują duże kontrowersje lub mają istotne znaczenie dla przyszłego kształtu przepisów o ochronie danych osobowych w Europie.

2. Wizyta Delegacji Stałej Komisji Landtagu Badenii-Wirtembergii

W dniu 24 czerwca 2013 r. w Biurze GIODO odbyło się spotkanie Generalnego Inspektora Ochrony Danych Osobowych z delegacją Stałej Komisji Landtagu Badenii-Wirtembergii. Podczas tego spotkania dr Wojciech Rafał Wiewiórowski, GIODO, przedstawił prezentację na temat działalności Generalnego Inspektora Ochrony Danych Osobowych na arenie krajowej i międzynarodowej

3. Wizyta przedstawicieli Urzędu Rzecznika Ochrony Prywatności Kanady

27 września 2013 r. odbyło się w Warszawie spotkanie Generalnego Inspektora Ochrony Danych Osobowych z przedstawicielami Urzędu Rzecznika Ochrony Prywatności Kanady. Podczas tej wizyty przedstawiciele kanadyjskiego i polskiego organu ochrony danych przedstawili informacje na temat działań swoich urzędów oraz wymienili się doświadczeniami. Przedmiotem dyskusji były kwestie dotyczące legislacji i orzecznictwa, działań informacyjno-edukacyjnych, spraw międzynarodowych, a także uprawnień organów

ochrony danych w zakresie kontroli, regulacji i zapewniania zgodności z przepisami o ochronie danych.

9.3. Międzynarodowe warsztaty

a) Warsztaty projektu PHAEDRA (Warszawa, 24 września 2013 r.)

Pierwsze warsztaty projektu badawczego Unii Europejskiej PHAEDRA, skierowanego na poprawę współpracy i koordynacji między organami ochrony danych i prywatności, odbyły się 24 września 2013 r. w Warszawie, podczas 35. Międzynarodowej Konferencji Rzeczników Danych Osobowych i Prywatności, której organizatorem był Generalny Inspektor Ochrony Danych Osobowych.

W warsztatach uczestniczyło ponad 70 przedstawicieli organów ochrony danych osobowych (DPAs), rzeczników ds. ochrony prywatności (PCs), organów ds. egzekwowania ochrony danych osobowych i prywatności (PEAs) oraz innych podmiotów zajmujących się problematyką prawa do prywatności i ochrony danych osobowych z całego świata. Przedstawiciele konsorcjum projektu złożonego z czterech partnerów z Polski, Belgii, Zjednoczonego Królestwa oraz Hiszpanii, zaprezentowali dotychczasowe rezultaty projektu, tj. wstępną wersję raportu podsumowującego studia przypadków i prezentującego analizę wyników badań ankietowych przeprowadzonych wśród przedstawicieli organów ochrony danych osobowych (na podstawie 53 odpowiedzi na ankietę) oraz podsumowanie wywiadów przeprowadzonych z wybranymi przedstawicielami DPAs, PCs i PEAs. Zaprezentowany też został wstępny raport ukazujący różnice w prawie do prywatności i ochrony danych osobowych między poszczególnymi krajami. Uczestnicy warsztatów wysłuchali 8 prezentacji przedstawicieli organów ochrony danych osobowych i prywatności na temat możliwości wzmocnienia współpracy i koordynacji wspólnych działań wszystkich zainteresowanych podmiotów. Istotnym elementem tego spotkania była również dyskusja na temat przyszłych kierunków działań konsorcjum na nadchodzący 2014 r. Największy nacisk położony został na identyfikację barier ograniczających współpracę i koordynację działań w obszarze egzekwowania prawa do prywatności i ochrony danych osobowych oraz opracowanie wytycznych co do strategii, które służyłyby zmniejszeniu i likwidacji tych barier. Podkreślono również potrzebę przygotowania ram wsparcia do wymiany informacji, wspólnych kontroli oraz innych skoordynowanych działań.

b) Warsztaty rozpatrywania spraw (Sarajewo, 2-3 października 2013 r.)

Pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych systematycznie uczestniczą w warsztatach rozpatrywania spraw, tzw. warsztatach skargowych (case handling workshop), które 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 25. warsztatach rozpatrywania skarg, zorganizowanych w dniach 2-3 października 2013 r. w Sarajewie przez Agencję Ochrony Danych Osobowych w Bośni i Hercegowinie[414]. Poszczególne sesje warsztatów dotyczyły tematów związanych z działalnością mediów, zapewnieniem prywatności w Internecie (ochrona danych dzieci, cloud computing, portale społecznościowe, itp.), bezpieczeństwa danych przetwarzanych w sektorze policyjnym, a także zagadnień komunikacji elektronicznej, marketingu bezpośredniego (w szczególności outsourcingu usług marketingowych), wideonadzoru w sektorze publicznym i prywatnym, oraz przetwarzania danych biometrycznych.

c) **Warsztaty TAIEX[415]** (Skopje, 29-30 maja 2013 r.)

GIODO uczestniczył w projekcie TAIEX „Civil & Criminal Liability for violating the right to personal data protection", zorganizowanym z inicjatywy Wydziału ds. Rozwoju Instytucjonalnego Dyrekcji Generalnej ds. Rozszerzenia (Institution Building Unit of the European Commission's Directorate General for Enlargement) oraz Rzecznika Ochrony Danych Osobowych w Byłej Jugosłowiańskiej Republice Macedonii. Warsztaty odbyły się w dniach 29-30 maja 2014 r. w Skopje. Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych przedstawił prezentację na temat orzecznictwa Europejskiego Trybunału Praw Człowieka w kontekście krajowego ustawodawstwa o ochronie danych osobowych.

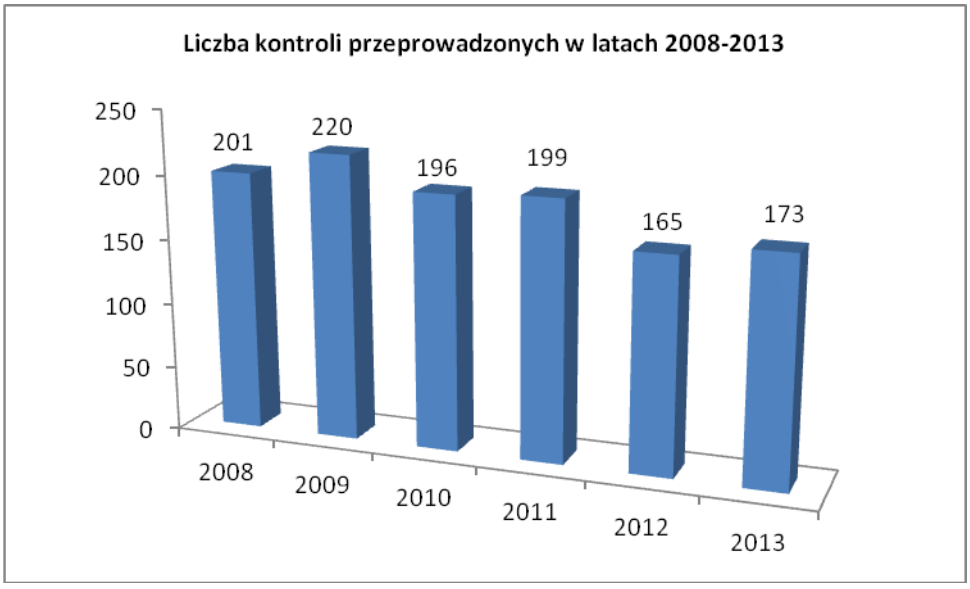
[414] zob. http://azlp.gov.ba/workshop/default.aspx/

[415] TAIEX – Technical Assistance and Information Office – jest instrumentem pomocy technicznej skierowanym do instytucji publicznych, które podejmują działania eksperckie w zakresie dostosowania ustawodawstwa swojego kraju do legislacji unijnej. Działania te mogą przybierać formę konferencji, seminariów, szkoleń, warsztatów czy wizyt studyjnych. TAIEX finansowany jest ze środków Komisji Europejskiej (http://taiex.ec.europa.eu/).

Wśród innych tematów poruszanych podczas tych warsztatów znalazły się zagadnienia związane z odpowiedzialnością cywilną za zniewagę i zniesławienie oraz ograniczenia wolności wypowiedzi i dostępu do informacji, a także kwestie związane z wdrożeniem art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności (prawo do poszanowania życia prywatnego i rodzinnego). Ponadto porównano doświadczenia poszczególnych państw w zakresie odpowiedzialności karnej i cywilnej za naruszenie prawa do ochrony danych osobowych.

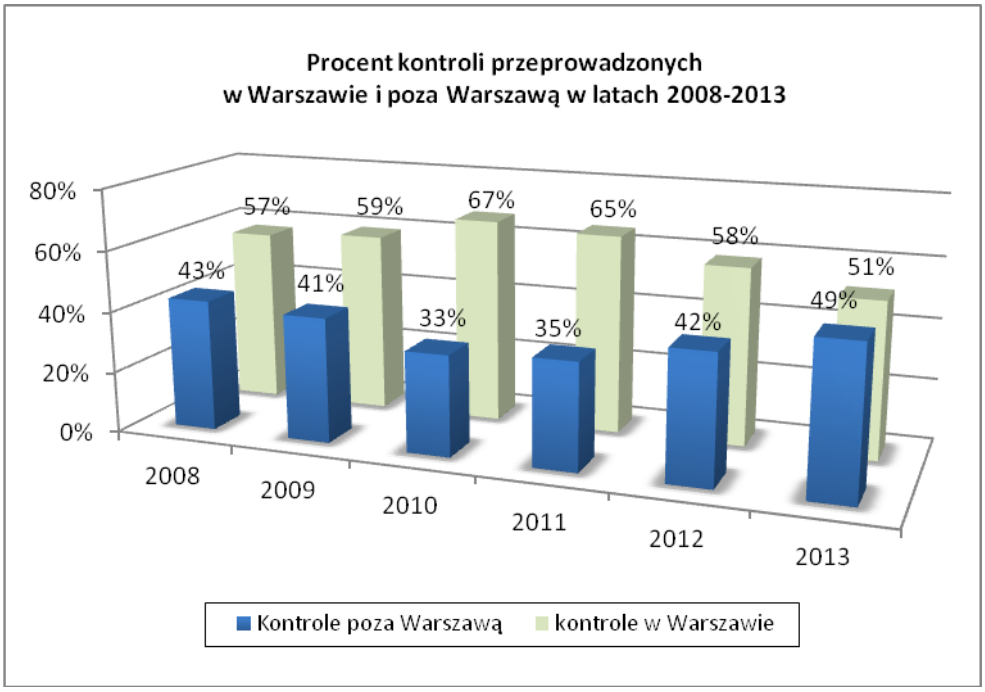
Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2013 roku

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 2012 liczba przeprowadzonych kontroli nieznacznie wzrosła ze 165 do 173.



Wykres 39: ***Porównanie liczby kontroli przeprowadzonych w latach 2008–2013.***

W analizowanym 2013 roku na ogólną liczbę 173 kontroli, 89 z nich przeprowadzonych było w Warszawie (51%), zaś 84 poza Warszawą (49%).



Wykres 40: ***Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2008–2013.***

Najwięcej kontroli przeprowadzonych zostało z urzędu (71). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący.

Inicjatywa kontroli	Liczba kontroli
Z urzędu	71
Departament Orzecznictwa, Legislacji i Skarg	49
Departament Rejestracji Zbiorów Danych Osobowych	11
Zespół ds. Naruszeń Danych Osobowych	6
Departament Edukacji Społecznej i Współpracy Międzynarodowej	3
Zespół ds. Egzekucji Administracyjnej	3
Zespół Rzecznika Prasowego	1
Prokuratura	6
Najwyższa Izba Kontroli	6
Rzecznik Praw Obywatelskich	4
W związku z inną kontrolą	13
RAZEM	**173**

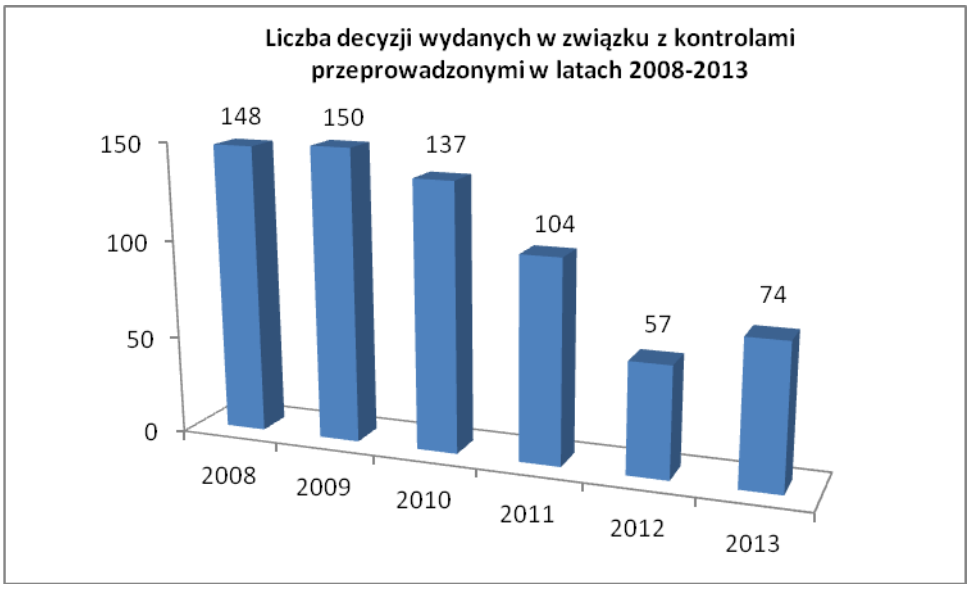
Czynnościom kontrolnym poddane zostały m.in. jednostki Policji, podmioty przetwarzające dane osobowe w związku z wykorzystaniem technologii identyfikacji radiowej – RFID, podmioty prowadzące programy lojalnościowe, jednostki samorządu terytorialnego w związku z realizacją obowiązków wynikających z ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. z 2012 r. poz. 391 z późn. zm.).

Spośród 173 kontroli przeprowadzonych w 2013 roku, **61 należało do kategorii kontroli sektorowych**. Dotyczyły one zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz przepisami innych ustaw obowiązujących w podmiotach należących do danego sektora.

Kontrolą sektorową objęto jednostki Policji w związku z wykorzystywaniem systemu informatycznego o nazwie „e-Posterunek", stanowiącego narzędzie służące do prowadzenia w wersji elektronicznej postępowań przygotowawczych przez Policję (7 kontroli), podmioty przetwarzające dane osobowe w związku z wykorzystaniem technologii identyfikacji radiowej – RFID (8 kontroli), podmioty prowadzące programy lojalnościowe (7 kontroli), jednostki samorządu terytorialnego w związku z realizacją obowiązków wynikających z ustawy o utrzymaniu czystości i porządku w gminach (15 kontroli) oraz podmioty prowadzące serwisy internetowe (10 kontroli). Ich wyniki zobrazowały sposób podejścia do problematyki ochrony danych osobowych oraz pozwoliły na sformułowanie wniosków co do zasad i sposobu przetwarzania danych osobowych przez podmioty należące do danego sektora.

W okresie sprawozdawczym, w związku z obecnością Polski w strefie Schengen, przeprowadzono kontrole przetwarzania danych osobowych w Krajowym Systemie Informatycznym (KSI) umożliwiającym organom administracji publicznej i organom wymiaru sprawiedliwości wykorzystywanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym. W sumie przeprowadzono 14 takich kontroli.

W 2013 r. Generalny Inspektor w związku z przeprowadzonymi kontrolami wydał **74 decyzje administracyjne,** skierował do organów ścigania **jedno zawiadomienie o podejrzeniu popełnienia przestępstwa** określonego w ustawie o ochronie danych osobowych, oraz **13 wystąpień do organów państwowych i organów samorządu terytorialnego**, w tym 9 wystąpień w trybie określonym w art. 19a ustawy o ochronie danych osobowych.



Wykres 41: ***Porównanie liczby decyzji wydanych w związku z kontrolami przeprowadzonymi w latach 2008–2013.***

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 obowiązek ten 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 umieszczeniu tych informacji w ramach 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 danych. W toku kontroli stwierdzano bowiem, iż administratorzy danych, pomimo istnienia przepisów prawa określających w sposób szczegółowy sposób przetwarzania danych osobowych, w tym dopuszczalny zakres ich zbierania, 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, które miało charakter istotnego naruszenia, gdyż było związane z pozyskaniem danych objętych szczególną ochroną na gruncie przepisów o ochronie danych osobowych. Administratorzy danych w dalszym ciągu mieli 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, zabraniem przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także z prawidłowym opracowaniem dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń i kategorii danych objętych ochroną, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Liczne uchybienia występowały również w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych. Trudności z prawidłowym wypełnieniem obowiązków określonych w przepisach rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, miały podmioty z większości sektorów opisanych w niniejszym *Sprawozdaniu*.

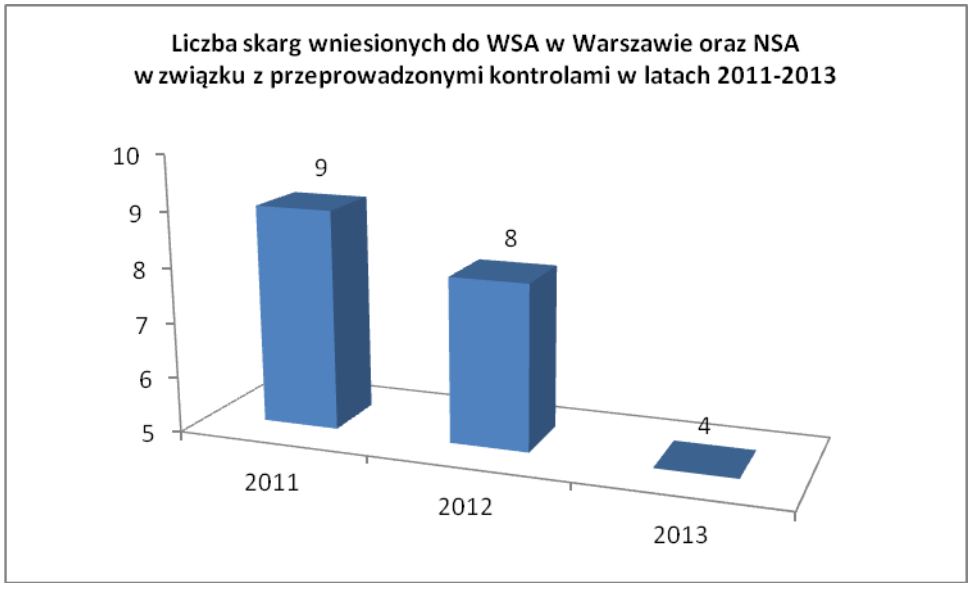
Obowiązki określone w przepisach o ochronie danych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Częstą przyczyną był również, jak wskazywali administratorzy danych, brak odpowiednich środków finansowych, 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 2013 r. kontroli były podmioty, dla których ochrona przetwarzanych danych osobowych jest ważnym zagadnieniem. Stosowane przez nie zasady przetwarzania danych osobowych odpowiadały wymogom wynikającym z przepisów o ochronie danych osobowych.

Na podstawie przeprowadzonych czynności kontrolnych należy również stwierdzić, że w części podmiotów objętych kontrolą, dokumenty zawierające dane osobowe przesyłane były za pośrednictwem sieci Internet, przy użyciu standardowych narzędzi poczty elektronicznej, tj. w sposób niezabezpieczony przed utratą poufności i integralności danych.

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 związku ze złożonymi skargami na decyzje wydane w latach 2011-2012 na skutek przeprowadzonych kontroli, sądy administracyjne wydały 6 orzeczeń, w tym 2 orzeczenia - Wojewódzki Sąd Administracyjny w Warszawie, zaś 4 orzeczenia - Naczelny Sąd Administracyjny. Natomiast w analizowanym 2013 r. do sądów administracyjnych wniesione zostały 4 skargi na decyzje GIODO w związku z przeprowadzonymi kontrolami.



Wykres 42: ***Zestawienie porównawcze liczby skarg wniesionych do Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2011-2013.***

Do istotnych orzeczeń, jakie zapadły w okresie sprawozdawczym w sprawach, w których przeprowadzane były kontrole, należy wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 kwietnia 2013 r. (sygn. akt II Sa/Wa 211/13). W wyroku tym sąd przychylił się do stanowiska Generalnego Inspektora wyrażonego w decyzji skierowanej do prezydenta miasta, w której nakazano m.in. zgłoszenie do rejestracji zbioru danych osobowych przetwarzanych w systemie informatycznym służącym do prowadzenia monitoringu miejskiego. W uzasadnieniu wyroku WSA w Warszawie stwierdził, iż straż miejska, realizując uprawnienia ustawowe do obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych przy użyciu środków technicznych, przetwarza w ramach monitoringu wizyjnego dane osobowe w postaci wizerunków (obrazów) osób przebywających w miejscach objętych zasięgiem monitoringu, a także inne informacje dotyczące tych osób, takie jak sposób zachowania czy numery rejestracyjne pojazdów. Dane te prowadzą do identyfikacji osoby, a zatem są to dane osobowe w rozumieniu art. 6 ustawy o ochrony danych osobowych. Jak podkreślił sąd, dane zarejestrowane w ramach monitoringu wizyjnego dostępne są według dwóch kryteriów: czasu oraz miejsca zdarzenia, tożsamego z miejscem umieszczenia kamery.

Na uwagę zasługuje również wyrok Naczelnego Sądu Administracyjnego z dnia 14 marca 2013 r. (sygn. akt I OSK 1059/12), w którym sąd przychylił się do stanowiska Generalnego Inspektora, wyrażonego w decyzji skierowanej do wspólnoty mieszkaniowej, nakazującej opracowanie i wdrożenie polityki bezpieczeństwa oraz wyznaczenie administratora bezpieczeństwa informacji. W uzasadnieniu wyroku NSA stwierdził, iż wspólnota mieszkaniowa, którą stanowi ogół właścicieli lokali wchodzących w skład określonej nieruchomości, jest administratorem danych dotyczących tych osób, zobowiązanym zastosować takie środki techniczne i organizacyjne, które zapewniają ochronę przetwarzania danych osobowych. Jeżeli administrator danych powierzył przetwarzanie danych innemu podmiotowi, to w myśl art. 31 ust. 4 ustawy o ochronie danych osobowych[416] odpowiedzialność w dalszym ciągu spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z umową.

W podsumowaniu na podstawie ustaleń z kontroli przeprowadzonych w 2013 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.

Innym negatywnym zjawiskiem zaobserwowanym w 2013 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

[416] Zgodnie z art. 31 ust. 4 ustawy o ochronie danych osobowych, w przypadku powierzenia przetwarzania danych odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

oczekiwania na osoby dysponujące wiedzą o procesie przetwarzania danych osobowych w celu przyjęcia od nich do protokołu ustnych wyjaśnień i na dokumenty mające bezpośredni związek z przedmiotem kontroli. Należy oczekiwać, że powyższy stan rzeczy będzie jednak ulegał stopniowej poprawie z uwagi na istnienie sankcji karnych za udaremnianie lub utrudnianie inspektorowi wykonania czynności kontrolnej[417].

Natomiast odnosząc się do charakterystyki **pytań prawnych** kierowanych do Generalnego Inspektora Ochrony Danych Osobowych w 2013 r. ich zakres tematyczny – podobnie jak w latach poprzednich - pozostawał bardzo szeroki i dotyczył wielu aspektów przetwarzania 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. Niemniej jednak można wskazać te zagadnienia, które pozostają, podobnie jak w latach ubiegłych, nadal aktualne. Dotyczyły one w szczególności:

1) **administracji** – szczególnie interesujące i liczne były kwestie przetwarzania danych związane z utrzymaniem czystości i porządku w gminach; w dalszym ciągu wiele wątpliwości dotyczyło również udostępniania informacji publicznej;
2) **banków** – w przedmiocie legalności przetwarzania danych osobowych klientów, w szczególności aspektów związanych z okresem przetwarzania danych, archiwizacją, marketingiem i dochodzeniem roszczeń wynikających z zawartych umów;
3) **służby zdrowia** – w odniesieniu do podstaw przetwarzania danych o stanie zdrowia, w tym udostępnienia takich danych przez podmioty lecznicze innym podmiotom, obowiązków podmiotów leczniczych związanych z przetwarzaniem danych pacjentów, właściwego zabezpieczenia dokumentacji medycznej oraz przypadków zagubienia dokumentacji medycznej;
4) **zatrudnienia –** w zakresie dopuszczalnego zakresu danych oraz przesłanek legalizujących wykorzystywanie danych przez pracodawców, działalności **związków zawodowych,** pośrednictwa pracy oraz prawidłowego zabezpieczenia danych osobowych;

[417] Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

wiele kontrowersji wzbudzało także przetwarzanie danych biometrycznych w stosunkach zatrudnienia;

5) **mieszkalnictwa –** zapytania dotyczące zarządzania nieruchomościami, w tym lokalami komunalnymi, wspólnotami mieszkaniowymi oraz administrowania spółdzielnią mieszkaniową.

6) **Internetu** - w tym w szczególności pozyskiwania danych osób - autorów wpisów na forum internetowym - celem ochrony własnych dóbr osobistych, przetwarzania danych w chmurze (*cloud computing*), przechowywania informacji w postaci plików *cookies* oraz niezamówionej informacji handlowej (spamu).

Część zapytań dotyczących działalności podmiotów publicznych koncentrowała się też na zagadnieniach właściwego realizowania obowiązków wynikających z ustawy o ochronie danych osobowych, w tym w szczególności obowiązku zapewnienia bezpieczeństwa danym osobowych przechowywanym na różnych nośnikach.

Tak jak w poprzednich latach działalności Generalnego Inspektora Ochrony Danych Osobowych, również w 2013 r. **przetwarzanie danych osobowych w związku z działalnością bankową** stanowiło częsty i istotny temat kierowanych do tego organu zapytań. Przedmiotem wątpliwości były w dalszym ciągu zasadnicze kwestie z tego zakresu, jak podstawy prawne i zakres pozyskiwania i dalszego przetwarzania danych osobowych przez banki i inne podmioty wykonujące działalność bankową, a także dopuszczalność przekazywania danych przez banki innym podmiotom, zasady prowadzenia czynności windykacyjnych czy uprawnienie do wykonywania kopii dowodu osobistego.

Ponadto klienci zgłaszali również zastrzeżenia, co do możliwości dysponowania przez bank ich danymi osobowymi w celach marketingowych mimo rozwiązania umowy z bankiem. Klienci banków często błędnie przyjmowali, że odstąpienie od umowy rachunku oznacza, że bank powinien definitywnie usunąć ich dane osobowe z prowadzonych przez siebie zbiorów. Organ ochrony danych osobowych w tego typu przypadkach wskazywał na art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych oraz na przepisy szczególne w stosunku do tej ustawy, które regulują przetwarzanie danych, np. przepisy z ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2009 r. Nr 152 poz. 1223).

W zakresie spraw dotyczących **ochrony zdrowia i przetwarzania danych przez podmioty lecznicze** wiele pytań dotyczyło podstaw przetwarzania danych o stanie zdrowia, w tym udostępnienia ich przez podmioty lecznicze innym podmiotom, obowiązków

podmiotów leczniczych związanych z przetwarzaniem danych pacjentów, właściwego zabezpieczenia dokumentacji medycznej oraz przypadków jej zagubienia.

Natomiast **zapytania dotyczące przetwarzania danych osobowych osób pozostających w stosunku zatrudnienia** dotyczyły takich zagadnień, jak dopuszczalnego zakresu danych oraz przesłanek legalizujących wykorzystywanie danych przez pracodawców, działalności związków zawodowych, pośrednictwa pracy oraz prawidłowego zabezpieczenia danych osobowych. Wiele kontrowersji wzbudzało także przetwarzanie w stosunkach zatrudnienia danych biometrycznych. W wielu sprawach, w których dane biometryczne wykorzystywane były np. do prowadzenia ewidencji czasu pracy, Generalny Inspektor uznawał za uzasadnione bliższe zbadanie sprawy poprzez przeprowadzenie czynności kontrolnych[418].

Problematyka opinii prawnych sporządzonych w 2013 r. obejmowała również zagadnienia związane z **działalnością spółdzielni oraz wspólnot mieszkaniowych** w przedmiocie przetwarzania danych osobowych, w tym podstaw prawnych upubliczniania danych ich członków (w szczególności w kontekście zaległości we wnoszeniu opłat), legalności systemu monitoringu na osiedlach czy rejestracji zbioru danych użytkowników parkingu. W odniesieniu do praktyki udostępnianie danych osobowych związanych z zaległościami czynszowymi poprzez ich ujawnianie w postaci różnego rodzaju list i zestawień wywieszanych w ogólnie dostępnych miejscach, np. na klatkach schodowych, Generalny Inspektor Ochrony Danych Osobowych wskazywał na możliwość rozważania złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa do organów ścigania.

Podsumowując działalność Generalnego Inspektora Ochrony Danych Osobowych w zakresie interpretacji przepisów prawa dotyczących problematyki ochrony danych osobowych stwierdzić należy, że zapotrzebowanie na taką formę działalności nie tylko nie słabnie, ale od kilku lat ma stałą tendencję wzrostową.

Działalność ta niewątpliwie przyczynia się do upowszechniania wśród ogółu obywateli znajomości zagadnień ochrony prywatności i danych osobowych, a co za tym idzie – wpływa na wzrost świadomości prawnej w tym zakresie. Często okazywało się również, że niezbędne jest podejmowanie interwencji przez Generalnego Inspektora Ochrony Danych Osobowych np. w formie wystąpień do administratorów danych w sytuacji zagrożenia dla praw

[418] DOLiS-035-2804/13, DOLiS-035-2805/13, DOLiS-035-3624/13

i wolności, które mogą wynikać zarówno z nieznajomości i nieprzestrzegania przez nich podstawowych zasad i obowiązków wynikających z przepisów o ochronie danych osobowych, jak i niewłaściwego korzystania z nowych technologii. Impulsem dla wystąpień Generalnego Inspektora Ochrony Danych Osobowych z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych do właściwych organów, były w dalszym ciągu braki lub istotne niedoskonałości w regulacjach prawnych w dziedzinie ochrony prywatności.

W ramach realizacji swoich ustawowych uprawnień oraz mając na uwadze potrzebę ciągłego doskonalenia ochrony danych osobowych, Generalny Inspektor Ochrony Danych Osobowych kieruje **wystąpienia do podmiotów publicznych i prywatnych, sygnalizując w nich konieczność zmiany stosowanych przez te podmioty praktyk, poprzez dostosowanie działań tych podmiotów do obowiązujących w zakresie ochrony danych osobowych przepisów prawa.** Wystąpienia Generalnego Inspektora mogą mieć charakter generalny bądź też stanowić reakcję na zgłoszenia indywidualnych osób, sygnalizujących Generalnemu Inspektorowi praktyki godzące w ich prywatność. Wskazywanie podmiotom podlegającym ustawie o ochronie danych osobowych właściwego sposobu stosowania jej przepisów, zapobiega ich naruszeniom i przyczynia się do podniesienia poziomu ochrony danych osobowych w Polsce.

W analizowanym roku 2013 Generalny Inspektor Ochrony Danych Osobowych wystosował **121 wystąpień, z czego 66 skierowanych zostało do podmiotów sektora prywatnego, a 55 – do publicznego.**

W analizowanym 2013 roku, źródłem wystąpień GIODO 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.

Natomiast w sytuacji wystosowania do podmiotów sektora prywatnego wystąpień na podstawie art. 19a ustawy, wobec stwierdzenia nieprawidłowości w procesie przetwarzania danych osobowych, podmioty te zawsze odpowiadały na skierowane do nich sygnalizacje.

W odpowiedzi informowały o podjętych lub planowanych działaniach mających na celu wyeliminowanie zasygnalizowanych nieprawidłowości. Wskazywały przy tym, iż respektowanie przez nie zasad wynikających z przepisów ustawy o ochronie danych osobowych pozwoli na uniknięcie ewentualnych zarzutów odnoszących się do przetwarzania danych osobowych osób, których dane dotyczą.

Podsumowując, Generalny Inspektor Ochrony Danych Osobowych w swoich wystąpieniach często zwracał uwagę, że zarówno podmioty prywatne, jak i publiczne, generalnie mają tendencję do zbierania jak najwięcej informacji o obywatelach. Przypominał jednak, że art. 51 ust. 2 Konstytucji RP wprost stanowi, że władza publiczna może gromadzić o obywatelu tylko te informacje, które są niezbędne w demokratycznym państwie prawnym. Nie ma zatem prawa zbierać informacji na zapas, które mogą być jej „przydatne", „potrzebne", „logiczne" czy „ekonomicznie opłacalne". Tak postanowiono w 1997 r. uchwalając Konstytucję i była to reakcja na państwo totalitarne. Pamięć państwa totalitarnego powinna być wciąż żywa w społeczeństwie, ponieważ dane zebrane nawet do zacnych celów, mogą zostać niewłaściwie wykorzystane przez instytucje prywatne i państwowe. Generalnego Inspektora Ochrony Danych Osobowych niepokoi na przykład brak niezależnego organu, który miałby możliwość dostępu do danych gromadzonych przez Policję i służby specjalne w celu sprawdzenia, czy podejmują one inwigilację i czy jest to zgodne z prawem oraz czy np. prowadzą przesiewowe badania Internetu. Pozyskiwanie przez demokratyczne państwo informacji o obywatelach powinno być ograniczone do niezbędnego minimum i podlegać kontroli niezależnego organu. Dlaczego z zadowoleniem przyjęta została informacja od Ministra Spraw Wewnętrznych o planowanym powołaniu organu, który będzie sprawował kontrolę nad Policją i służbami specjalnymi, aby w Polsce nie doszło do wielkiej elektronicznej inwigilacji obywateli na wzór tej, prowadzonej w Stanach Zjednoczonych z wykorzystaniem programu PRISM, czy rosnącej kontroli obywateli przez organy podatkowe oraz służby specjalne. GIODO niezmiennie podkreśla, że szeroki dostęp do danych powinien zostać zapewniony o ile jest to związane z toczącym się postępowaniem w sprawie. Natomiast przesiewowe badanie obywateli, np. pod kątem prowadzonych operacji finansowych jest niedopuszczalne.

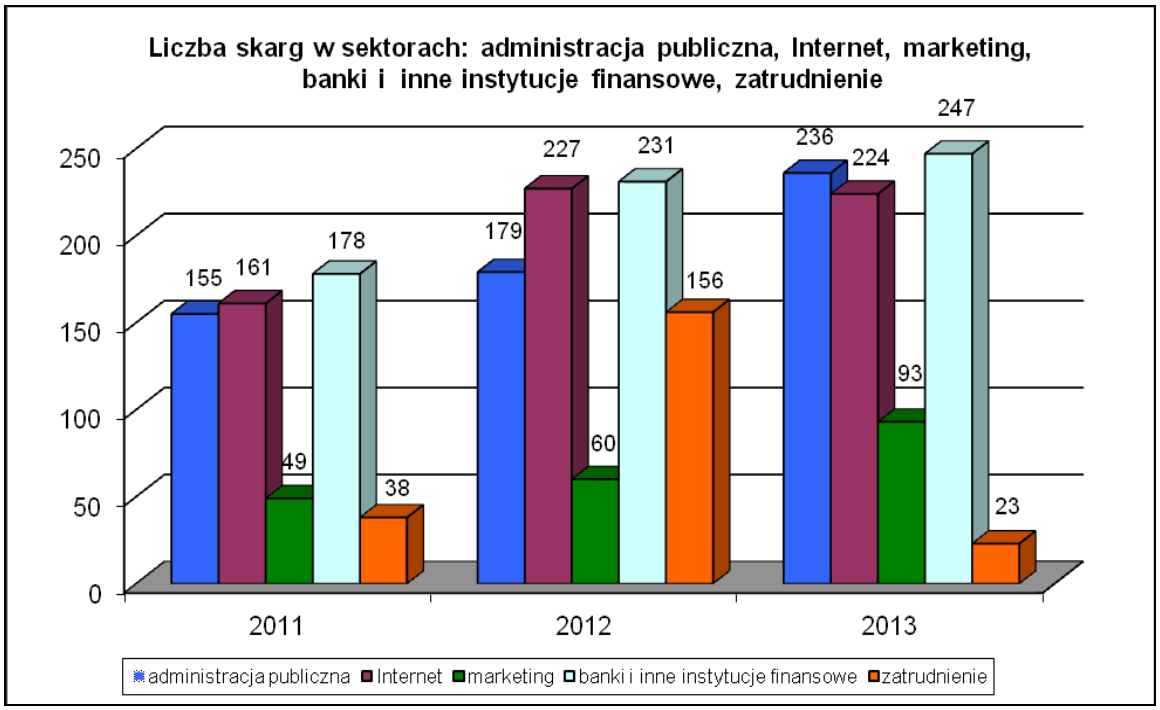
W porównaniu z poprzednimi latami, w 2013 r. można zauważyć systematyczny od kilku lat **wzrost liczby skarg,** które wpływają do Biura GIODO. W roku 2009 wpłynęło 1049

skarg, w 2010 – 1114, w 2011 – 1271, w 2012 – 1593, zaś **w 2013 - 1879**. Przyczyn tego stanu należy upatrywać przede wszystkim we wzroście świadomości obywateli co do zasad ochrony danych osobowych i ich aktywności w dochodzeniu przysługujących im 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 2012-2013 pozwala zauważyć pewne inne interesujące trendy. Pierwszym z nich był znaczący wzrost liczby skarg w sektorze administracji publicznej (rok 2012 - 179, rok 2013 - 236), w sektorze marketingu (rok 2012 - 60, rok 2013 - 93) oraz w sektorze odnoszącym się do działalności banków i innych instytucji finansowych (rok 2012 - 231, rok 2013 - 247). 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, poprzez 231 skarg w 2012, zaś w 2013 wynosiła już 247.

Interesujący trend można zaobserwować w odniesieniu do sektora zatrudnienia, w którym w latach 2011-2012 nastąpił ponad czterokrotny wzrost liczby skarg - z 38 skarg w 2011 r. do 156 w 2012 r. Natomiast w analizowanym 2013 r. mamy 23 skargi na podmioty tego sektora, co oznacza prawie siedmiokrotny ich spadek w stosunku do roku 2012.

W niektórych sektorach liczba skarg jest co roku na porównywalnym poziomie, tj. w sektorze telekomunikacyjnym (rok 2012- 91, rok 2013 - 86), w sektorze dotyczącym mieszkalnictwa (rok 2012 – 88, rok 2013 - 93) oraz w sektorze działalności ubezpieczeniowej (rok 2012- 24, rok 2013 - 37). Podkreślenia natomiast wymaga, że w odniesieniu do podmiotów sektora związanego z działalnością internetową liczba skarg utrzymuje się – co prawda – na porównywalnym z poprzednimi latami poziomie, aczkolwiek jest to wciąż wysoki poziom (rok 2012- 227, rok 2013 - 224).



Wykres 43: ***Porównanie liczby skarg w sektorach: administracja publiczna, Internet, banki i inne instytucje finansowe, marketing i zatrudnienie w latach 2011–2013.***

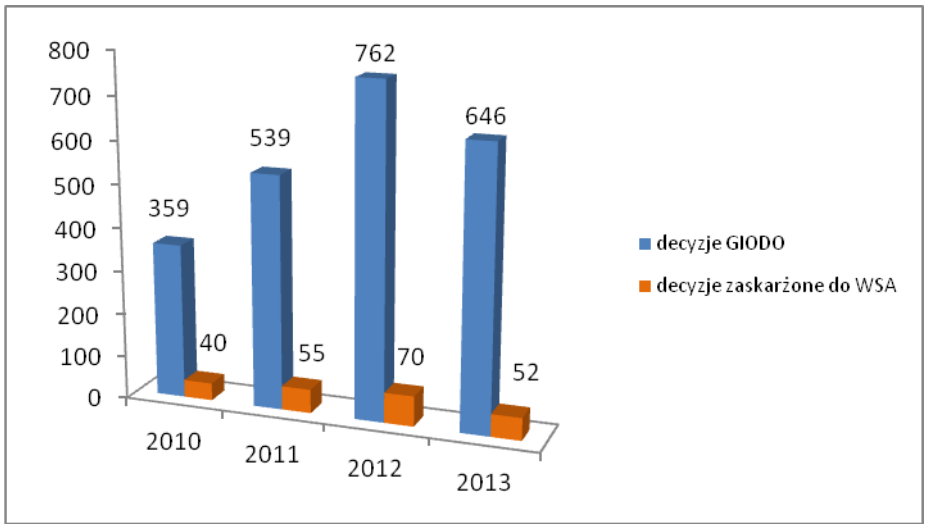
W podsumowaniu należy zauważyć, że systematycznie poprawia się poziom przetwarzania danych osobowych przez administratorów danych, którzy – jak wynika z podejmowanych przez nich działań – współdziałają z organem ochrony danych osobowych w celu wypracowywania lepszych standardów ochrony danych. W wielu sprawach bowiem, po interwencji Generalnego Inspektora, podejmowali oni odpowiednie działania zmierzające do zmian kwestionowanych praktyk.

Odnosząc się do faktu corocznego wzrostu liczby 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 GIODO zmierzającej do upowszechnienia wiedzy o prawach i obowiązkach zarówno administratorów danych, jak i osób, których dane dotyczą.

Na konieczność odpowiedniej ochrony danych osobowych wskazują 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.

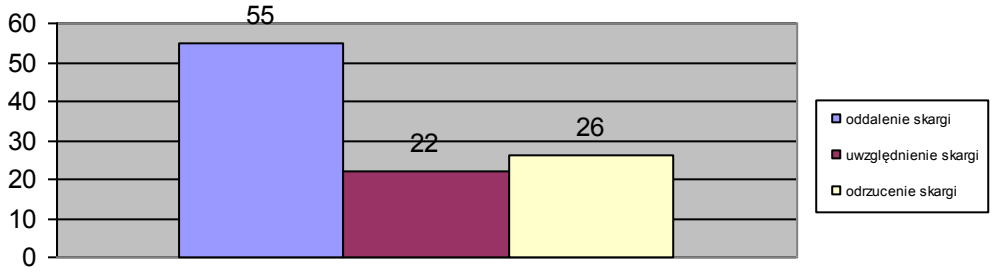
Odnosząc się zaś do zakresu tematycznego skarg rozpatrywanych w omawianym 2013 roku, zasadniczo nie zauważa się znaczących zmian. W porównaniu z rokiem 2012 problemy pojawiające się we wpływających w 2013 r. do Biura GIODO wnioskach uznać należy za tożsame. Jednocześnie wskazać należy, iż część tych skarg dotyczyła bieżących problemów prawnych, jak np. tzw. ustawy śmieciowej czy też zagadnień związanych z Centralnym Wykazem Ubezpieczonych – elektroniczną weryfikacją uprawnień świadczeniobiorców.

W postępowaniach zainicjowanych skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych w 2013 roku z urzędu, wydanych zostało **646 decyzji administracyjnych,** z których **52** zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie (WSA). W porównaniu z rokiem 2012, w którym 70 decyzji zostało zaskarżonych, oznacza to spadek o 18 spraw.



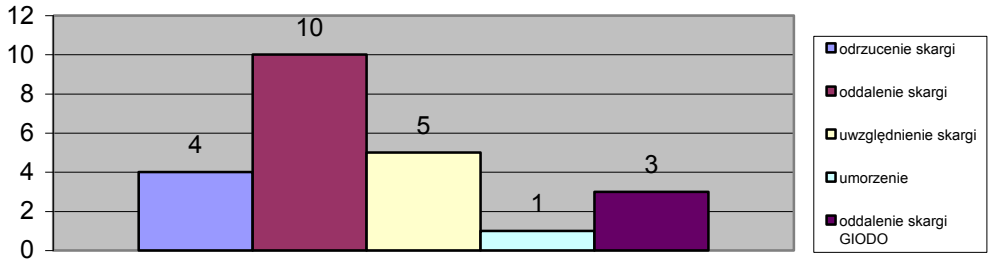
Wykres 44: ***Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2013 w związku z rozpatrywanymi skargami.***

Spośród 223 orzeczeń wydanych w 2013 roku w sprawach związanych ze skargami, 126 orzeczeń rozstrzygało sprawy co do istoty, zaś pozostałe 97 stanowiły orzeczenia wydawane w toku prowadzonych przez sądy administracyjne postępowań. Przy czym WSA w Warszawie rozstrzygał sprawy co do istoty w 103 przypadkach, zaś Naczelny Sąd Administracyjny wydał 23 orzeczenia orzekające co do istoty wniesionych skarg kasacyjnych, co ilustrują poniższe wykresy.



Wykres 45: ***Orzeczenia WSA w Warszawie wydane w 2013 r. w sprawach skarg prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych.***

Wśród orzeczeń wydanych przez WSA w 2013 r. w **55** przypadkach sąd orzekł o **oddaleniu** skargi na decyzję GIODO, zaś w **22** przypadkach **uchylił** zaskarżone decyzje. Ponadto w **26** sprawach WSA orzekł o **odrzuceniu** skargi spowodowanym nieuzupełnieniem, we wskazanym przez sąd terminie, braków formalnych złożonych skarg.



Wykres 46: ***Orzeczenia NSA wydane w 2013 r. w związku ze skargami kasacyjnymi wniesionymi od wyroków WSA w Warszawie.***

Wśród wyroków, które zapadły w wyniku skargi podmiotów na decyzje organu ds. ochrony danych osobowych, należy w szczególności wskazać **na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 lipca 2013 r. (sygn. akt II SA/Wa**

815/13) na decyzję GIODO[419] w sprawie odmowy uwzględnienia wniosku w sprawie skargi na przetwarzanie danych osobowych skarżącego przez sądy rejonowe. W wyroku tym podkreślone zostało, że: „*W rozpoznawanej sprawie nie ulega wątpliwości, że doszło do naruszenia ustawy o ochronie danych osobowych, czego nie kwestionuje Generalny Inspektor Ochrony Danych Osobowych, jednakże skarżący nie przyjmuje argumentów Generalnego Inspektora Ochrony Danych Osobowych, co do możliwości jego działania określonych w art. 12 przedmiotowej ustawy. W ocenie Sądu, skarżący fakt niewykorzystania przysługujących mu praw wynikających z powyżej określonych ustaw procesowych i ustrojowych dotyczących toczących się, czy też zakończonych postępowań karnych »przenosi« na Generalnego Inspektora Ochrony Danych Osobowych, a w szczególności domaga się podjęcia działań, łącznie z zawiadomieniem prokuratury o zaistniałym, w jego ocenie przestępstwie*". Ponadto Sąd wskazał, że: *„(...) skoro skarżący dowiedział się o zaistnieniu przestępstwa ściganego z urzędu, to na nim ciążył przede wszystkim obowiązek zawiadomienia organy ścigania. Skarżący obowiązku tego nie dopełnił i niezasadnie czyni z tego tytułu zarzut Generalnemu Inspektorowi Ochrony Danych Osobowych. Reasumując, Sąd stwierdza, że podnoszone w skardze zarzuty nie mogły zostać uwzględnione, gdyż Generalny Inspektor Ochrony Danych Osobowych w zakresie przyznanych mu przez ustawodawcę kompetencji dopełnił ciążące na nim obowiązki, a co więcej - wyszedł poza ich zakres określony art. 12 ustawy o ochronie danych osobowych, który stanowi katalog otwarty w podejmowaniu działań zmierzający do ochrony danych osobowych. Wystąpienie Generalnego Inspektora Ochrony Danych Osobowych do Ministra Sprawiedliwości związanego ze stwierdzonymi uchybieniami w zakresie przetwarzania danych osobowych skarżącego, Sąd ocenia jako wypełnienie ustawowego obowiązku tego organu. Ponadto Sąd w pełni podziela stanowisko organu w zakresie dochodzenia przez skarżącego jego praw dotyczących ewentualnego naruszenia jego dóbr osobistych, ale w tym zakresie powinien działać sam, bez wykorzystywania organu, który realizuje określone w ustawie o ochronie danych osobowych zadania".*

Na uwagę zasługuje także **wyrok Naczelnego Sądu Administracyjnego z dnia 21 sierpnia 2013 r. (sygn. akt I OSK 1666/12), w którym wskazał, iż z brzmienia art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną wynika jedynie obowiązek udzielenia informacji o danych organom państwa na potrzeby prowadzonych przez nie**

[419] Decyzja GIODO z dnia 5 marca 2013 r. DOLiS/DEC-263/13/13825,13830,13832.

postępowań. Nie wynika natomiast zakaz udostępniania tych danych osobom, których prawa zostały naruszone. Zarówno jednak organ nakazujący ujawnienie danych, jak i sąd administracyjny rozpoznający skargę na tego rodzaju decyzję, muszą każdorazowo, przy uwzględnieniu indywidualnych okoliczności danej sprawy dokonać wyważenia przeciwstawnych interesów, jakimi są prawo do ochrony danych osobowych i prawo do ochrony czci, godności, dobrego imienia czy też wizerunku firmy. Należy przy tym w sposób należyty uwzględniać wymogi wynikające z zasady proporcjonalności, tak aby stosowane środki były adekwatne do zagrożenia dobra wymagającego w danej sprawie większej ochrony. Wyrażony pogląd jest zgodny z normami konstytucyjnymi, a zwłaszcza z art. 31 ust. 2 i 3 Konstytucji RP, z którego wynika, że każdy jest obowiązany szanować wolności i prawa innych, a ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane w ustawie i tylko wtedy gdy są konieczne m.in. dla ochrony wolności i praw innych osób. Przepisy ustawy o ochronie danych osobowych pozwalające na ujawnienie tych danych we wskazanych w ustawie przypadkach są właśnie takim wyjątkiem pozwalającym osobie, której prawa naruszono, dochodzić ochrony należnej jej w demokratycznym państwie.

Naczelny Sąd Administracyjny podkreślił, iż w obecnie obowiązującym stanie prawnym można wysnuć wniosek, iż w ramach obowiązującego prawa, pod pewnymi warunkami, można domagać się ujawnienia danych, jakie zgromadził administrator serwisu internetowego poprzez stosowanie mniej restrykcyjnej ustawy niż ustawy o świadczeniu usług drogą elektroniczną, czyli ustawy o ochronie danych osobowych, a konkretnie art. 23 tej ustawy. Warunkami tymi są proporcjonalność środków i celów oraz równowaga pomiędzy ochroną różnych dóbr: wolności wypowiedzi i prawa do ochrony dóbr osobistych. Podmiot żądający udostępnienia danych osobowych musi swoje stanowisko uzasadnić. W świetle art. 23 ust. 1 pkt 5 muszą być to „prawnie usprawiedliwione cele". W przypadku odmowy udostępnienia danych przez podmiot będący ich administratorem, strona może złożyć wniosek do Generalnego Inspektora, który po przeprowadzeniu stosownego postępowania może w drodze decyzji nakazać udostępnienie danych osobowych. Istotna w tym zakresie jest ocena Generalnego Inspektora Ochrony Danych Osobowych, która powinna być uzależniona od okoliczności konkretnej sprawy, bowiem zarówno ustawa o świadczeniu usług drogą elektroniczną, jak i ustawa o ochronie danych osobowych będą miały w tym zakresie zastosowanie. Podejmując decyzję Generalny Inspektor Ochrony Danych Osobowych musi

w każdej indywidualnej sprawie ocenić, które dobra chronione przez prawo są ważniejsze – dane osobowe czy interes gospodarczy przedsiębiorstwa.

W oparciu o omówiony powyżej wyrok WSA Generalny Inspektor Ochrony Danych Osobowych umocnił swój pogląd dotyczący tego, iż art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną nie wyklucza stosowania ustawy o ochronie danych osobowych i tym samym nie wyłącza możliwości udostępnienia danych podmiotom innym niż wskazane w tym przepisie.

W 2013 r. roku **Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę na decyzję Generalnego Inspektora Ochrony Danych Osobowych[420] wydaną w sprawie wniosku o wydanie decyzji administracyjnej nakazującej usunięcie danych osobowych skarżącego zawartych w odpowiedzi Prokuratora Krajowego, zastępcy Prokuratora Generalnego, na interpelację zamieszczoną przez Kancelarię Sejmu na stronie internetowej.** Generalny Inspektor decyzją odmówił uwzględnienia wniosku, a następnie po złożeniu wniosku o ponowne rozpatrzenie sprawy utrzymał zaskarżoną decyzję w mocy[421].

WSA w przedmiotowym wyroku wskazał, że cyt.: *„W ocenie Sądu, należy zgodzić się z organem, że przetwarzanie danych osobowych skarżącego przez Kancelarię Sejmu w związku z realizacją obowiązku wynikającego zarówno z Konstytucji RP, a następnie z Regulaminu Sejmu, oparte było o przesłanki legalizujące przetwarzanie tych danych osobowych określone w art. 23 ust. 1 pkt 2 ustawy. (...) W ocenie Sądu, Kancelaria Sejmu należycie wywiązała się ze spoczywającego na niej obowiązku przetwarzania danych adekwatnych w stosunku do celów, w jakich są przetwarzane. Adekwatność danych w stosunku do celu ich przetwarzana winna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi a interesem administratora danych. Równowaga jest zachowana, gdy administrator przetwarza dane osobowe tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia prawnie usprawiedliwionego celu. Administrator danych nie może w żaden sposób stawiać swego interesu ponad dobro osoby, której dane przetwarza. (...) Pozyskanie danych winno być ściśle determinowane celem, jakiemu ma służyć. W ocenie Sądu rozpoznającego sprawę zakres udostępnionych, a dotyczących skarżącego, informacji nie wykracza poza niezbędny dla realizacji celu jakim*

[420] Wyrok WSA w Warszawie z dnia 25 października 2013 r. sygn. akt II SA/Wa 998/13.
[421] Decyzja GIODO z dnia 9 października 2012 r. DOLiS/DEC-964/12/61068,61070.
Decyzja GIODO z dnia 2 kwietnia 2013 r. DOLiS/DEC-377/13/20496,20509.

jest ogłaszanie w Systemie Informacyjnym Sejmu treści odpowiedzi na interpelację. Ponadto zgodzić się należy z organem, że Regulamin Sejmu nie ogranicza prawa do informacji publicznej ze względu na prywatność osoby fizycznej, jak również nie odsyła do art. 5 ust. 2 ustawy o dostępie do informacji publicznej. Reasumując stwierdzić należy, iż organ prawidłowo ustalił, że w niniejszej sprawie wystąpiły przesłanki legalizujące przetwarzanie danych osobowych skarżącego przez Kancelarię Sejmu, określone w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych".

W innej sprawie, wyrokiem z dnia 14 marca 2013 r. (sygn. akt I OSK 620/12) Naczelny Sąd Administracyjny oddalił skargę kasacyjną Wójta Gminy W. od wyroku WSA z dnia 24 listopada 2011 r. (sygn. akt II SA/Wa 1828/11). NSA w ww. wyroku podkreślił, iż: *„Badając zgodność z prawem przetwarzania danych osobowych (...) prawidłowo zarówno Generalny Inspektor jak i Sąd pierwszej instancji posłużyły się zasadami określającymi dopuszczalność przetwarzania danych osobowych zamieszczonych w art. 23 ust. 1 ustawy, przyjmując, że przesłanka legalizująca przetwarzanie tych danych była wymieniona w pkt 2 powołanego przepisu. Dopuszcza on przetwarzanie danych osobowych, jeżeli jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W niniejszej sprawie obowiązkiem wynikającym z przepisu prawa było zamieszczenie przez Wójta Gminy informacji o treści uchwały Rady Gminy w urzędowym publikatorze teleinformacyjnym – Biuletynie Informacji Publicznej. Do spełnienia tego obowiązku nie było niezbędne ujawnienie danych osoby fizycznej, która wniosła skargę na działalność Wójta Gminy. Jeżeli celem zamieszczenia informacji publicznej w BIP-ie jest transparentność działalności publicznej Rady Gminy, w tym treść podejmowanych przez nią uchwał, to cel ten zostaje spełniony także wówczas, gdy chroniąc sferę prywatności z informacji usunięte zostaną dane dot. osób prywatnych. Należy zważyć, iż skarga (...) dotyczyła niewłaściwego załatwiania przez Wójta Gminy spraw indywidualnych, w tym przewlekłego załatwiania jego pism. Uznanie przez Radę Gminy skargi (...) za niezasadną z podaniem obszernego uzasadnienia obrazującego jednoznacznie rodzaj spraw, w których obywatel kwestionował prawidłowość działania organu, nie uzasadniało posłużenia się w informacji zamieszczonej w BIP-ie pełnym imieniem i nazwiskiem. Stanowisko Generalnego Inspektora uznające, że w procesie przetwarzania danych osobowych obywatela skarżącego się na działalność organu doszło do naruszenia prawa i wydania decyzji na podstawie art. 18 ust. 1 pkt 6 ustawy nakazującej usunięcie ze strony internetowej BIP danych osobowych (...) w zakresie imienia*

i nazwiska z uchwały Rady Gminy W. (...) nie naruszało prawa. Zamieszczenie w uzasadnieniu decyzji wzmianki o możliwości anonimizacji danych nie stanowiło konkretyzacji nakazu zawartego w osnowie decyzji, lecz przykładowo wskazywało na możliwe sposoby działania organu w takim przypadku. Nie można zatem przypisać Generalnemu Inspektorowi naruszenia prawa przez nałożenie obowiązku nieistniejącego w przepisach prawa, gdyż treść nałożonego na organ obowiązku odpowiada ściśle określonemu w art. 18 ust. 1 pkt 6 ustawy, który to przepis został powołany w podstawie prawnej decyzji."

W wyroku tym NSA wskazał na słuszność praktyki orzeczniczej stosowanej przez Generalnego Inspektora Ochrony Danych Osobowych w prowadzonych przez niego postępowaniach administracyjnych.

Analizując z kolei działalność **opiniotwórczą** Generalnego Inspektora Ochrony Danych Osobowych w 2013 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.

Jak już była o tym mowa, w 2013 r. zgłoszonych zostało do **rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych 28264 zbiory, z czego 15304 zbiory pochodziły od podmiotów publicznych, zaś 12960 od podmiotów prywatnych.**

W przypadku sektora prywatnego, w roku sprawozdawczym zanotowano znaczący wzrost liczby zgłoszeń zbiorów danych osobowych przesyłanych przez przedsiębiorców, którzy przetwarzając dane osobowe wykorzystują Internet. Natomiast wśród zgłoszeń do rejestracji pochodzących od podmiotów publicznych w roku 2013 r. (podobnie jak w roku 2012) stosunkowo dużą liczbę stanowiły zbiory danych osobowych zgłaszane do rejestracji przez przedszkola i szkoły.

Wśród podmiotów z sektora publicznego należy wskazać na znaczną liczbę zgłoszeń zbiorów prowadzonych przez gminy na podstawie przepisów ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. z 2013 r. poz. 1399 z późn. zm.). Były to np. zbiory danych osobowych dotyczące prowadzenia ewidencji zbiorników bezodpływowych czy przydomowych oczyszczalni ścieków. Jak już była o tym mowa w innej części *Sprawozdania*, po nowelizacji dokonanej ustawą z dnia 1 lipca 2011 r. o zmianie ustawy o utrzymaniu czystości i porządku w gminach oraz niektórych innych ustaw (Dz. U. Nr 152, poz. 897), gminy zobowiązane zostały do zorganizowania odbierania odpadów komunalnych od właścicieli nieruchomości. Natomiast właścicieli nieruchomości zobligowano do złożenia do wójta, burmistrza lub prezydenta miasta deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w terminie 14 dni od dnia zamieszkania na danej nieruchomości pierwszego mieszkańca lub powstania na danej nieruchomości odpadów komunalnych. Znowelizowana ustawa zobowiązała radę gminy do określenia wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanej przez właściciela nieruchomości, nie wskazała natomiast zakresu danych osobowych, jakie mogą być pozyskiwane za jej pomocą. Określając, w drodze uchwały, wzór deklaracji rada gminy wskazała w konsekwencji także zakres danych osobowych pozyskiwanych za jej pomocą przez gminę.

Z treści zgłoszeń nadsyłanych do rejestracji wynikało m.in., że niektóre gminy wymagały podania w deklaracji danych osób zamieszkujących wspólnie z właścicielem lub załączenia do deklaracji dokumentów potwierdzających stałą nieobecność osoby zameldowanej pod danym adresem. W ten sposób mogły zostać pozyskane np. informacje

o pobycie takiej osoby w zakładzie karnym lub zakładzie opieki zdrowotnej. Wątpliwości budził też zakres pozyskiwanych danych o właścicielach nieruchomości[422].

Natomiast w przypadku wielu zbiorów dotyczących składanych deklaracji o wysokości opłaty za odpady zgłoszonych do rejestracji na podstawie przepisów ww. ustawy, konieczne było przeprowadzenie postępowania wyjaśniającego dotyczącego zakresu danych zawartych w deklaracjach. W odpowiedzi na wezwanie do złożenia wyjaśnień administratorzy danych często informowali o ograniczeniu zakresu pozyskiwanych do zbioru danych osobowych. Niekiedy administratorzy wskazywali, że zgłoszony do rejestracji zbiór obejmuje nie tylko deklaracje o wysokości opłaty za odpady, ale również np. dane przetwarzane w związku z naliczaniem i pobieraniem opłat.

W roku sprawozdawczym do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zgłaszane były również zbiory danych osobowych przetwarzanych w związku z funkcjonowaniem funduszy inwestycyjnych i emerytalnych, w szczególności zbiory danych dotyczących członków funduszy oraz osób, których dane są 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, pełnomocnicy), dłużników wierzytelności nabytych przez fundusz sekurytyzacyjny, a także osób, do których kierowane były różnego rodzaju działania marketingowe. Przy rozpatrywaniu tego typu zgłoszeń kluczową kwestią jest ustalenie, czy w świetle przepisów ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Dz. U. Nr 146, poz. 1546 z późn. zm.) oraz ustawy z dnia z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (Dz. U. z 2010 r. Nr 34, poz. 189 z późn. zm.) regulujących działalność funduszy inwestycyjnych i emerytalnych, status administratora danych przetwarzanych w danym zbiorze zgłoszonym do rejestracji, przysługuje funduszowi inwestycyjnemu albo emerytalnemu, czy też towarzystwu funduszy inwestycyjnych albo emerytalnemu. W przepisach regulujących funkcjonowanie ww. podmiotów przyjęta została bowiem konstrukcja prawna, zgodnie z którą fundusz inwestycyjny i fundusz emerytalny posiadają osobowość prawną, ale zarządzane i reprezentowane są odpowiednio przez towarzystwo funduszy inwestycyjnych albo towarzystwo emerytalne stanowiące odrębną

[422] W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych skierował w dniu 27 maja 2013 r. wystąpienie do Ministra Administracji i Cyfryzacji, wskazując na opisane uchybienia w zakresie pozyskiwania przez gminy danych osobowych za pomocą deklaracji o wysokości opłat za gospodarowanie odpadami komunalnymi (DOLiS-072-12/13).

osobę prawną. Poza tym istnieją odrębne regulacje odnoszące się do poszczególnych rodzajów funduszy. Typowym przykładem jest odmienność regulacji w zakresie prowadzenia rejestru uczestników funduszu inwestycyjnego otwartego i ewidencji uczestników funduszu inwestycyjnego zamkniętego. Zgodnie bowiem z art. 87 ustawy o funduszach inwestycyjnych, rejestr uczestników funduszu inwestycyjnego otwartego prowadzi ten fundusz. Natomiast podmiotami uprawnionymi do prowadzenia ewidencji uczestników funduszu inwestycyjnego zamkniętego są: towarzystwo zarządzające tym funduszem, Krajowy Depozyt Papierów Wartościowych Spółka Akcyjna lub spółka, której przekazał on wykonywanie czynności z zakresu zadań, o których mowa w art. 48 ust. 1 pkt 1 lub 2 ustawy o obrocie instrumentami finansowymi, dom maklerski, bank krajowy lub instytucja kredytowa (art. 123 ust. 4 ustawy o funduszach inwestycyjnych).

Uznając za rozstrzygającą treść przepisów ww. ustaw, które wyznaczają rolę funduszu inwestycyjnego lub emerytalnego i towarzystwa funduszy inwestycyjnych lub emerytalnych 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, Generalny Inspektor Ochrony Danych Osobowych stanął na stanowisku, iż to fundusz inwestycyjny lub emerytalny jest administratorem tych danych osobowych, które przetwarzane są w celu realizacji uprawnień i obowiązków funduszu inwestycyjnego lub emerytalnego wynikających z ustawy o funduszach inwestycyjnych lub ustawy o organizacji i funkcjonowaniu funduszy emerytalnych.

Należy zwrócić uwagę, że towarzystwa funduszy inwestycyjnych i towarzystwa emerytalne są administratorami danych osobowych m.in. w przypadku, jeśli przetwarzają dane w związku z realizacją własnych zadań ustawowych lub 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. Z tego też powodu do ogólnokrajowego rejestru wpisywane zostały prowadzone przez towarzystwa funduszy inwestycyjnych - zgodnie z art. 123 ustawy o funduszach inwestycyjnych - zbiory danych stanowiące ewidencję uczestników funduszy inwestycyjnych zamkniętych, czy też zbiory danych służące celom marketingowym. Stanowisko w tej kwestii Generalny Inspektor Ochrony Danych Osobowych podtrzymał także w przygotowanych w roku sprawozdawczym trzech odpowiedziach na skargi kasacyjne od

wyroków Wojewódzkiego Sądu Administracyjnego[423] oddalających skargi jednego z towarzystw emerytalnych.

Na uwagę zasługuje również przykład zbioru danych klientów korzystających z usług w zakresie preparatyki i przechowywania materiału genetycznego, zgłoszonego w 2013 r. do rejestracji GIODO[424]. Na potrzeby przechowywania próbek biologicznych tworzone są biobanki, które mają bardzo różną formę prawną i są wykorzystywane do różnych celów. Jedna z działających w Polsce Spółek postanowiła świadczyć usługi w zakresie separacji i przechowywania próbek DNA i zgłosiła do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych ww. zbiór zawierający dane klientów.

Przy rozpatrywaniu przedmiotowej sprawy powstały wątpliwości, czy administrator danych (Spółka) w związku z realizacją umowy o izolację, preparatykę i przechowywanie materiału genetycznego, przechowując próbki DNA będzie przetwarzać dane osobowe, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych. W nadesłanym do rejestracji zgłoszeniu Spółka nie poinformowała o zamiarze przetwarzania takich danych, a w toku postępowania twierdziła, iż materiał genetyczny może być przedmiotem własności podobnym do rzeczy i jego ochrona przed niedozwolonymi ingerencjami osób trzecich powinna być wywodzona z przepisów prawa rzeczowego. Tym samym Spółka kwestionowała stosowanie przepisów o ochronie danych osobowych „do tkanek, które nie są same w sobie danymi osobowymi".

Generalny Inspektor Ochrony Danych Osobowych stanął na stanowisku, że przechowywanie próbek DNA jest przetwarzaniem danych osobowych szczególnie chronionych, tj. danych o kodzie genetycznym i stanie zdrowia. Pozyskiwane przez spółkę próbki DNA mogą być bowiem wykorzystywane do diagnostyki medycznej, a w konsekwencji istnieje też możliwość ustalenia już istniejącej choroby. W tym kontekście Generalny Inspektor Ochrony Danych Osobowych podkreślił, że nie może również budzić wątpliwości, że usługa świadczona przez Spółkę na rzecz jej klientów ma na celu właśnie umożliwienie pozyskania informacji genetycznej i informacji o stanie zdrowia. Wobec poczynionych przez inspektorów Biura GIODO ustaleń, że Spółka posiada podstawę do przetwarzania danych szczególnie chronionych, kluczową dla GIODO była kwestia

[423] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 20 listopada 2012 r. (sygn. akt II SA/Wa 1474/12), wyroki Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 stycznia 2013 r. (sygn. akt II SA/Wa 1475/12, sygn. akt II SA/Wa 1476/12).
[424] Zgłoszenie nr R 007643/11

powierzenia przetwarzania danych osobowych w zgłoszonym do rejestracji zbiorze. Czynności kontrolne wykazały bowiem, iż z materiału pobranego od klienta sporządzane będą dwie próbki DNA. Jedną z próbek Spółka zamierzała przechowywać w siedzibie innego podmiotu zawierając z nim w tym celu ustną umowę. Biorąc pod uwagę, że Spółka zlecając wykonanie ww. czynności innemu podmiotowi powinna zawrzeć z tym podmiotem (pisemną) umowę powierzenia przetwarzania danych osobowych, spełniającą wymogi określone w art. 31 ustawy, Generalny Inspektor Ochrony Danych Osobowych odmówił rejestracji zbioru stwierdzając, że przetwarzanie danych osobowych klientów Spółki naruszałoby zasadę legalności (art. 26 ust. 1 pkt 1 w związku z art. 31 ust. 1 ustawy). Okoliczność ta stanowi zaś przesłankę odmowy rejestracji zbioru danych, o której mowa w art. 44 ust. 1 pkt 2 ustawy. Odmawiając rejestracji zwrócono uwagę, że umowa powierzenia przetwarzania danych osobowych powinna również obejmować, obok danych o kodzie genetycznym i stanie zdrowia, również niepowtarzalny kod, którym oznaczone będą próbki DNA.

Decyzja Generalnego Inspektora Ochrony Danych Osobowych stała się przedmiotem skargi rozpoznanej przez Wojewódzki Sąd Administracyjny w Warszawie. Sąd oddalił skargę potwierdzając, że Spółka przechowując próbki DNA w jednostce badawczej powinna zawrzeć z tym podmiotem umowę spełniającą wymogi określone w art. 31 ustawy, którą powierzyłaby mu przetwarzanie danych w zakresie informacji genetycznej, stanu zdrowia i kodu klienta, którym oznaczona będzie próbka. Sąd tym samym w pełni podzielił stanowisko Generalnego Inspektora Ochrony Danych Osobowych. To precedensowe rozstrzygnięcie będzie miało istotne znaczenie dla rozpatrywania podobnych spraw, których z pewnością będzie coraz więcej.

Rozwój nowych technologii i powszechny dostęp do Internetu przyczynił się do powstawania różnego rodzaju serwisów społecznościowych, w których użytkownicy chętnie zamieszczają zdjęcia, wpisy i inne treści, co skutkuje gromadzeniem ogromnej ilości informacji o osobach, w tym danych wrażliwych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych. Przedsiębiorcy dążą do komercyjnego wykorzystania informacji zawartych w tego typu serwisach, zwłaszcza poprzez świadczenie w oparciu o te dane własnych usług o charakterze marketingowym, czy badawczym. I tak, jedna ze spółek będąca właścicielem serwisu społecznościowego zgłosiła do rejestracji zbiór danych[425], który

[425] Zgłoszenie nr R 008290/12

miał obejmować przede wszystkim dane osobowe umieszczone w serwisie społecznościowym przez jego użytkowników. Zbiór ten miał służyć przede wszystkim prowadzeniu przekrojowych prac analitycznych i badawczych na potrzeby własne spółki, jak również być wykorzystywany w celu realizacji własnych usług specjalistycznych - badawczych, statystycznych i w ramach organizacji konkursów i - w jej zamiarze - pokrywać miał zapotrzebowanie rynkowe na tego typu usługi. Przewidywano przetwarzanie zarówno danych osobowych zwykłych jak również danych osobowych szczególnie chronionych, wymienionych w art. 27 ust. 1 ustawy. Spółka planowała pozyskiwanie odrębnej zgody na przetwarzanie danych w celach świadczenia usług specjalistycznych, badawczych, statystycznych i organizacji konkursów. Natomiast nie zamierzała pozyskiwać pisemnej zgody na przetwarzanie danych osobowych wymienionych w art. 27 ust. 1 ustawy, ponieważ - jej zdaniem - jest to niemożliwe w świecie cyfrowym (czyli w realiach usług świadczonych przez Spółkę). Jednocześnie Spółka podkreślała, że przesłanką przetwarzania przez nią tego rodzaju danych stanowi - w jej ocenie - art. 27 ust. 2 pkt 8 ustawy, tj. przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dotyczą.

Biorąc pod uwagę, że znaczna część procesów przetwarzania danych miała odbywać się w oparciu o ustawę o świadczeniu usług drogą elektroniczną, Generalny Inspektor Ochrony Danych Osobowych wskazał, że zgodnie z art. 16 ust. 1 ww. ustawy do przetwarzania danych osobowych w rozumieniu ustawy o ochronie danych osobowych, w związku ze świadczeniem usług drogą elektroniczną, stosuje się przepisy tej ustawy, o ile przepisy rozdziału 4 ustawy o świadczeniu usług drogą elektroniczną nie stanowią inaczej. Ustawa o świadczeniu usług drogą elektroniczną będzie więc stanowić *lex specialis* wobec przepisów ustawy, tym samym zaś wyłączać stosowanie jej przepisów wszędzie tam, gdzie stanowi regulacje odrębne.

W związku z powyższym, w zakresie w jakim do przetwarzania danych miałaby zastosowanie ustawa o świadczeniu usług drogą elektroniczną, zastosowanie znajduje przepis art. 18 tej ustawy, który stanowi, iż usługodawca może przetwarzać dane osobowe usługobiorcy niezbędne do ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi: nazwisko i imiona usługodawcy, numer ewidencyjny PESEL (lub gdy nie został on nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość), adres zameldowania na pobyt stały, adres do korespondencji, dane służące do weryfikacji podpisu elektronicznego usługobiorcy oraz adresy elektroniczne usługobiorcy. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca

może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia. Ponadto usługodawca może przetwarzać inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną, za zgodą usługobiorcy, dla celów określonych w art. 19 ust. 2 pkt 2 ustawy o świadczeniu usług drogą elektroniczną, tj. niezbędne do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę.

W konsekwencji Generalny Inspektor Ochrony Danych Osobowych wskazał, że art. 18 ust. 4 ustawy o świadczeniu usług drogą elektroniczną wyklucza, w odniesieniu do przetwarzania przez usługodawcę danych osobowych, które nie są niezbędne do świadczenia na rzecz danej osoby usługi drogą elektroniczną, możliwość zastosowania określonych w art. 23 ust. 1 i 27 ust. 2 ustawy przesłanek legalności przetwarzania danych osobowych, innych niż zgoda osoby na przetwarzanie danych, które jej dotyczą. W przepisach rozdziału 4 ustawy o świadczeniu usług drogą elektroniczną nie została natomiast uregulowana forma wyrażenia zgody na przetwarzanie danych osobowych. W tym zakresie zastosowanie mają zatem przepisy ustawy o ochronie danych osobowych. Oznacza to, że do przetwarzania tzw. danych szczególnie chronionych określonych art. 27 ust. 1 ustawy konieczna jest zgoda wyrażona na piśmie. Zaznaczyć przy tym należy, że „wyrażenie zgody na piśmie", o którym stanowi art. 27 ust. 2 pkt 1 ustawy o ochronie danych osobowych, może nastąpić także poprzez złożenie oświadczenia w postaci elektronicznej opatrzonego bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu[426].

Niezależnie od omówionych wyżej przepisów ustawy o świadczeniu usług drogą elektroniczną i konsekwencji ich zastosowania, Generalny Inspektor Ochrony Danych Osobowych wskazał uzupełniająco, że przesłanka określona w art. 27 ust. 2 pkt 8 ustawy spełniona jest wyłącznie w przypadku, gdy dane osobowe są podane do publicznej wiadomości. Oznacza to, że istnieje możliwość zapoznania się z nimi przez niezamknięty, bliżej nieokreślony krąg osób. Nie ma natomiast charakteru podania do publicznej wiadomości informacja skierowana do ograniczonego grona określonej grupy osób. W przypadku, gdy użytkownicy serwisu społecznościowego zdecydują, jakie informacje o nich będą dostępne dla innych zarejestrowanych użytkowników, a jakie dane będą dostępne

[426] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, Warszawa 2011, s. 555.

wyłącznie dla ich znajomych, nie można uznać, że właściciel serwisu przetwarza dane podane do publicznej wiadomości.

Generalny Inspektor Ochrony Danych Osobowych rozpatrując sprawę wskazał również, że użytkownicy serwisu decydując się na umieszczenie w nim swoich danych, powinni mieć zaufanie, że ich dane będą ujawnione i wykorzystywane tylko w taki sposób, na jaki wyrazili wolę udostępniając je w serwisie. Korzystając z serwisu użytkownicy zmierzają do realizacji celów, którym on służy, a więc np. wyszukiwania znajomych oraz wymiany korespondencji, uwag i opinii, czy zawierania nowych znajomości. Przyjąć jednocześnie należy, że nie jest objęte wolą użytkownika serwisu umożliwienie nieograniczonemu kręgowi osób wykorzystywania jego danych osobowych w innych celach i na innych zasadach niż te, które związane były z jego decyzją o udostępnieniu dotyczących go wrażliwych danych osobowych. Przyjęcie, iż przesłanka określona w art. 27 ust. 2 pkt 8 ustawy legalizuje przetwarzanie przez Spółkę danych wrażliwych użytkowników prowadzonego przez nią serwisu w celu świadczenia własnych usług specjalistycznych - badawczych, statystycznych i w ramach organizacji konkursów - oznaczałoby, że każdy inny podmiot mógłby się w stosunku do użytkowników serwisu na tę przesłankę powołać. Nie trzeba przekonywać, że sytuacja, w której dane wrażliwe umieszczone w serwisie mogłyby być wykorzystywane w nieograniczony sposób, w dowolnym celu, nawet wbrew woli osób, których dotyczą, stwarzałaby poważne zagrożenie dla interesów użytkowników serwisu.

Generalny Inspektor Ochrony Danych Osobowych uznał więc, że przesłanka przetwarzania wrażliwych danych osobowych określona w art. 27 ust. 2 pkt 8 ustawy nie znajduje w opisanej sytuacji zastosowania. Zaprezentowane w omawianej sprawie stanowisko ma istotne znaczenie dla przypadków, w których przedsiębiorcy (zwłaszcza świadczący usługi w zakresie badań rynkowych, marketingu i reklamy) zamierzają wykorzystywać dane osobowe szczególnie chronione, które zostały zamieszczone w serwisach społecznościowych przez ich użytkowników.

Należy zwrócić również uwagę na zwiększającą się liczbę wpływających do Biura GIODO zgłoszeń zbiorów danych nadsyłanych do rejestracji przez podmioty publiczne, a dotyczących przetwarzania danych osobowych w megabazach tworzonych przez te podmioty. Przy rozpatrywaniu tego typu zgłoszeń powstaje szereg problemów związanych m.in. z ustaleniem, któremu organowi przysługuje status administratora danych przetwarzanych w zgłoszonym zbiorze (niejednokrotnie chodzi bowiem o bazy

wykorzystywane przez organy administracyjne różnych szczebli), określeniem podstawy prawnej lub zakresu danych, który jest adekwatny do celu przetwarzania danych w zbiorze. Problemy te powoduje zazwyczaj brak szczegółowych uregulowań prawnych dotyczących funkcjonowania określonego zbioru. W takich przypadkach podmiot zgłaszający zbiór, jako podstawę przetwarzania w nim danych osobowych wskazuje jedynie przepisy określające ogólnie jego kompetencje. Niejednokrotnie problemy wynikają również z niejasności przepisów odnoszących się do przetwarzania danych w zgłoszonym do rejestracji zbiorze.

Jako przykład tego typu zbiorów zgłoszonych do rejestracji w 2013 roku wskazać można zbiór danych osobowych o nazwie „BAZA DANYCH SIO”[427] prowadzony przez Ministra Edukacji Narodowej w oparciu o przepisy ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. Nr 139, poz. 814 z późn. zm.), czy systemy Syriusz i Viator[428] wspomagające pracę powiatowych i wojewódzkich urzędów pracy, których zgłoszenia dokonał Minister Pracy i Polityki Społecznej. W uregulowaniach prawnych dotyczących tych systemów brak precyzyjnych zapisów odnośnie roli i statusu Ministra Pracy i Polityki Społecznej, czy wskazania właściwego zakresu danych. Co więcej, w zgłoszeniach zbiorów pochodzących z urzędów pracy, Minister Pracy i Polityki Społecznej był nieraz wskazywany jako podmiot, któremu powierzono przetwarzanie danych osobowych w trybie art. 31 ustawy o ochronie danych osobowych. W przypadku tego typu zbiorów konieczne było przeprowadzenie postępowania wyjaśniającego, a często również czynności sprawdzających na miejscu.

W związku z planowaną w ramach projektu ustawy o ułatwieniu wykonywania działalności gospodarczej, nowelizacją ustawy o ochronie danych osobowych, która dotyczy m.in. uregulowania statusu i zadań administratorów bezpieczeństwa informacji, zgłaszania ich do rejestracji GIODO i nowych zwolnień w zakresie obowiązku zgłaszania zbiorów danych do rejestracji (w tym zwolnienia związanego z powołaniem i zgłoszeniem do rejestracji administratora bezpieczeństwa informacji), Generalny Inspektor Ochrony Danych Osobowych opracował projekt rozporządzenia w sprawie wzorów zgłoszeń powołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz odwołania administratora bezpieczeństwa informacji.

[427] Zgłoszenie nr R 000766/13
[428] Zgłoszenie nr R 012958/13 oraz zgłoszenie nr R 12911/13

W podsumowaniu podkreślenia wymaga, że na decyzje wydane w latach 2012-2013 w związku z rejestracją zbiorów danych osobowych, sądy administracyjne wydały w 2013 r. 3 orzeczenia. Natomiast w analizowanym 2013 r. do sądów administracyjnych wniesione zostały 4 skargi na decyzje GIODO w związku z rejestracją - 1 skarga do WSA w Warszawie i 3 skargi kasacyjne do NSA.

Ważną częścią działalności Generalnego Inspektora Ochrony Danych Osobowych jest **edukacja i podnoszenie świadomości społecznej** w sprawach dotyczących prawa do prywatności i ochrony danych osobowych. W ramach swoich kompetencji ujętych w art. 12 ustawy o ochronie danych osobowych, Generalny Inspektor prowadzi szeroko zakrojone działania informacyjno-edukacyjne i patronuje wielu wydarzeniom, których tematyka zbieżna jest z zakresem działań organu, wpływając w ten sposób na świadomość obywateli w kwestii bezpieczeństwa dotyczących ich danych osobowych. Uczestniczy w spotkaniach, konferencjach, seminariach i innych wydarzeniach w kraju i za granicą, organizowanych z inicjatywy jego, bądź innych podmiotów. Aktywnie angażuje się w liczne działania upowszechniające wiedzę, jak wydawanie publikacji, broszur, wywiady i konferencje prasowe, organizuje konkursy, bezpłatne szkolenia (w tym e-learningowe) i warsztaty adresowane głównie do przedstawicieli administracji rządowej i samorządowej oraz przedstawicieli instytucji publicznych. Współpracuje ze szkołami wyższymi, z którymi, w ramach zawartych porozumień, podejmuje różnego rodzaju inicjatywy, jak organizacja studiów podyplomowych, konferencji, debat i seminariów promujących tematykę prywatności i ochrony danych osobowych. W 2013 r. do grona tych szkół dołączył Uniwersytet Ekonomiczny w Poznaniu. Generalny Inspektor Ochrony Danych Osobowych współpracuje również z takimi podmiotami, jak organizacje pozarządowe, studenckie poradnie prawne i stowarzyszenia studenckie oraz samorządowe ośrodki doskonalenia zawodowego nauczycieli, w tym z Gliwickim Ośrodkiem Metodycznym w Gliwicach – GOM, który na zasadzie partnera metodycznego uczestniczy w organizowanym przez GIODO ogólnopolskim programie edukacyjnym „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli". W 2013 roku, do IV edycji tego edukacyjnego przedsięwzięcia, swój udział zgłosiło 139 placówek oświatowych. Na uwagę zasługują także cykliczne organizowane kampanie edukacyjne z okazji Dnia Ochrony Danych Osobowych, Dni Otwartych GIODO w różnych

częściach Polski, Tygodnia Zapobiegania Kradzieży Tożsamości czy Dnia Bezpiecznego Internetu, podczas których wspólnie z innymi podmiotami podejmowane są działania na rzecz ochrony prywatności i danych osobowych.

W ramach V edycji kampanii „Nie daj się okraść, chroń swoją tożsamość", w Akademii im. Leona Koźmińskiego w Warszawie, zorganizowane zostało Śniadanie Naukowe, podczas którego Generalny Inspektor Ochrony Danych Osobowych w wykładzie pt. „Zabezpieczenie danych. Dlaczego gubimy to, czego powinniśmy strzec?", uczulał studentów na niebezpieczeństwa związane z brakiem dbałości o ochronę dotyczących ich danych osobowych (25.10.2013 r.).

Ponieważ w ostatnich latach zasada odpowiedzialności i rozliczalności stała się jednym z ważniejszych wątków dyskusji o ochronie prywatności, zagadnienie to stało się tematem projektu realizowanego przez Centre for Information Policy Leadership (CIPL). Jego częścią było seminarium pt. „Accountability Phase V. The Essentials Elements in Distributed Environments" (Rozliczalność. Faza V. Elementy zasadnicze w środowiskach rozproszonych") współorganizowane przez GIODO (20-21.02.2013 r.). Podczas tego wydarzenia Generalny Inspektor omówił kwestię ryzyka oraz zastosowania zasady odpowiedzialności i rozliczalności w środowiskach rozproszonych, takich jak chmura publiczna czy aplikacje mobilne. W seminarium uczestniczyli przedstawiciele środowisk gospodarczych, nauki oraz organów ochrony danych osobowych. W ramach tego wydarzenia zorganizowane zostało również odrębne spotkanie skierowane do przedstawicieli organów ochrony danych osobowych z państw Europy Środkowej i Wschodniej.

W dobie dynamicznego rozwoju nowoczesnych technologii, Generalny Inspektor Ochrony Danych Osobowych podejmuje też kroki w celu bliższego poznania praktycznej strony realizacji różnych projektów. Przykładem może być wizyta GIODO i jego przedstawicieli w siedzibie spółki Energia Operator w Gdańsku (19.06.2013 r.), która wdrożyła system inteligentnego opomiarowania energii. Spotkanie to było okazją nie tylko do poznania sposobu gromadzenia i przechowywania informacji przekazywanych przez inteligentne liczniki energii i ich oględzin, ale także do omówienia zagadnień związanych z bezpieczeństwem danych osobowych pozyskiwanych za ich pośrednictwem.

Kontynuacją tego działania była debata przedstawicieli firm – dostarczycieli energii elektrycznej - oraz prawników z udziałem GIODO oraz prezesa Urzędu Regulacji Energetyki, która pod hasłem „Prywatność i dane osobowe w inteligentnych sieciach energetycznych"

odbyła się 26 czerwca 2013 r. w Warszawie. Spotkanie to było elementem szerszej dyskusji publicznej na temat inteligentnego opomiarowania, w szczególności aspektu gromadzenia danych pomiarowych i należytej ochrony prywatności odbiorców energii. Podczas debaty Generalny Inspektor Ochrony Danych Osobowych podkreślił, że dane pomiarowe są danymi osobowymi i dlatego bez zgody klienta zbierane powinny być tylko te, które służą zapewnieniu ciągłości dostaw, optymalizacji pracy sieci energetycznej i jej zarządzaniu oraz rozliczeniom za zużytą energię. Celem tego spotkania było przedstawienie stanowisk i wymiana informacji na temat wdrażanych systemów i technologii oraz dyskusja nad koniecznymi regulacjami prawnymi i ich możliwym kształtem. Dzisiejsze technologie niewątpliwie wyprzedzają rozwiązania prawne. Dlatego tak ważne jest wypracowanie rozwiązań, które realizując oczekiwania rynku zapewnią najwyższe standardy bezpieczeństwa danym osobowym.

Z doświadczeń Generalnego Inspektora Ochrony Danych Osobowych wynika również, że przedstawiciele sektora administracji publicznej nie zawsze wiedzą na co zwracać uwagę, rozważając możliwość skorzystania z usługi *cloud computingu*. Podpowiedzią dla nich był przygotowany przez GIODO i opublikowany na jego stronie internetowej dekalog chmuroluba[429]. Przedstawiono w nim 10 zasad, jakimi powinni kierować się administratorzy danych osobowych sektora administracji publicznej, w przypadku zawierania umów na usługi świadczone w chmurze obliczeniowej. Dekalog chmuroluba stanowi opracowanie informacji zawartych w różnych wystąpieniach i materiałach GIODO, grupujące wskazania dla tych, którzy - mimo wątpliwości - po przeprowadzeniu oceny wpływu działania na ochronę prywatności, decydują się na zastosowanie usług chmurowych w administracji publicznej.

GIODO podejmuje i wspiera także różne inne inicjatywy, mające na celu wzrost wiedzy obywateli w zakresie ochrony danych osobowych. W związku z rozwojem nowoczesnych technologii, zwłaszcza teleinformatycznych, szczególnie podkreśla konieczność współdziałania różnych środowisk w zakresie edukacji cyfrowej, na co zwróciła uwagę „Rezolucja w sprawie edukacji cyfrowej dla wszystkich", przyjęta podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności: Przewodnik Po Zagmatwanym Świecie, która odbyła się w dniach 23-26 września 2013 r. w Warszawie. Uchwalona wówczas została **Deklaracja Warszawska w sprawie upowszechniania się**

[429] http://www.giodo.gov.pl/259/id_art/6271/j/pl/

aplikacji w społeczeństwie[430], sygnowana przez Generalnego Inspektora Ochrony Danych Osobowych Wojciecha R. Wiewiórowskiego oraz Przewodniczącego Komitetu Wykonawczego Międzynarodowej Konferencji Jacoba Kohnstamma. W dokumencie tym rzecznicy zobowiązali się do zadbania o to, aby użytkownikom zapewnić lepsze doświadczenia w zakresie ochrony ich prywatności, poprzez bezpośrednie zwrócenie się do wszystkich interesariuszy w związku z ich rolą i zobowiązaniami w zakresie realizacji tego prawa – a więc do twórców aplikacji, dostawców systemów operacyjnych oraz rzeczników ochrony danych i prywatności.

W dniu 30 października 2013 r. Generalny Inspektor Ochrony Danych Osobowych wziął udział w debacie poświęconej roli podnoszenia świadomości obywateli w zakresie zarządzania prywatnością w sieci, w budowaniu zaufania i zachęcania ich do korzystania z udogodnień gospodarki cyfrowej. Debata towarzyszyła powołaniu **Partnerstwa dla zwiększenia świadomości i wiedzy obywateli na temat cyfrowej tożsamości**, które powstało m.in. z inicjatywy Ministerstwa Administracji i Cyfryzacji. Misją Partnerstwa, które jest formą współpracy między przedsiębiorcami, organizacjami społecznymi i instytucjami publicznymi, jest zwiększanie wiedzy obywateli o sposobach zarządzania prywatnością w sieci i świadomym – opartym na przejrzystych zasadach – wykorzystaniu cyfrowej tożsamości w celu rozwoju gospodarki internetowej. Generalny Inspektor Ochrony Danych Osobowych przystąpił do tej inicjatywy, która może przyczynić się do zwiększenia świadomości wśród użytkowników sieci oraz do budowania przez różne branże przyjaznych dla prywatności i bezpieczeństwa danych osobowych standardów postępowania. W 2014 roku planowane jest przeprowadzenie kampanii propagującej zasady budowania i ochrony cyfrowej tożsamości, a także publikacje raportów i organizacja konferencji dotyczących tożsamości cyfrowej, ochrony danych osobowych i prywatności w Internecie. Generalny Inspektor Ochrony Danych Osobowych jest również członkiem Komitetu Honorowego **Szerokiego Porozumienia na Rzecz Umiejętności Cyfrowych** - nieformalnego zrzeszenia instytucji, organizacji i firm, którego zadaniem jest wspieranie rozwoju kompetencji cyfrowych obywateli niezbędnych na rynku pracy i realizacji ich indywidualnych aspiracji. Realizację tego zadania można obecnie śmiało uznać za priorytet rozwojowy kraju.

[430] www.giodo.gov.pl/plik/id_p/5240/j/pl/

Ponadto GIODO prowadzi także z Ministerstwem Administracji i Cyfryzacji skoordynowane działania w ramach projektu budowy elektronicznej platformy służącej do zgłaszania incydentów związanych z rasizmem i ksenofobią, o czym była już mowa w innej części niniejszego *Sprawozdania*.

W 2013 r. Generalny Inspektor Ochrony Danych Osobowych kontynuował również prace merytoryczne w obszarze **monitoringu**. Przedstawiciele GIODO aktywnie uczestniczyli w spotkaniach roboczych organizowanych przez Ministerstwo Spraw Wewnętrznych, w związku z przygotowywaniem założeń do projektu ustawy o monitoringu. Kontynuowane były też prace w zakresie **inteligentnego pomiaru** i związanych z tym zagrożeń prywatności. Rezultatem tych prac był artykuł pod tytułem „Smart metering – ochrona danych osobowych", opublikowany w „IT w Administracji - miesięcznik informatyków i menadżerów IT sektora publicznego".

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

Rozwój gospodarki cyfrowej opartej na danych udostępnionych w sieci powoli staje się faktem. Przepływ danych i informacji w Internecie stał się siłą napędową rozwoju społecznego i ekonomicznego. Gospodarkę tę tworzą nie tylko firmy obecne w Internecie, ale także inne podmioty – konsumenci i internauci, którzy biorą aktywny udział w cyfrowym życiu społecznym, kulturalnym i gospodarczym. Większość konsumentów podkreśla, jak ważna jest dla nich ochrona prywatności oraz to, by wykorzystywanie informacji na ich temat przez inne podmioty odbywało się w sposób przejrzysty, odpowiedzialny i kontrolowany. Wzrasta więc świadomość obywateli w kwestii wykorzystania potencjału nowych technologii na poprawę jakości ich życia we wszystkich wymienionych wyżej obszarach, zaś transakcje przeprowadzane na pozbawionym granic jednolitym rynku cyfrowym pozwalają im docenić prawdziwą wartość Internetu. Dlatego przed organem ds. ochrony danych stoi wciąż bardzo ważne zadanie w kwestii związanej z zachęceniem administratorów danych do inwestowania, od początku, w prawidłową ochronę danych, np. poprzez realizację koncepcji ochrony

prywatności w fazie projektowania (privacy by design)[431], ustawień domyślnych (privacy by default), oceny wpływu na ochronę prywatności, a także wzrostu ich świadomości, co do odpowiedzialności i rozliczalności za przetwarzane przez nich dane osobowe przez cały cykl życia informacji.

Podkreślenia wymaga, że przepisy dotyczące ochrony danych osobowych często były wskazywane przez przedstawicieli przemysłu jako przeszkoda dla innowacji i rozwoju gospodarki. Peter Hustinx, Europejski Inspektor Ochrony Danych Osobowych (EIOD), w oświadczeniu prasowym z 29 maja 2013 r. odpowiedział na ten zarzut: *„Korzyści dla przemysłu nie powinny – i nie muszą – być osiągane kosztem naszych praw podstawowych do ochrony danych i prywatności. Uwzględnienie zasad ochrony danych w innowacjach technicznych oraz przy przekazywaniu naszych danych osobowych właściwym organom, np. w celu zapewnienia bezpieczeństwa, może stanowić istotną wartość dodaną, zarówno jeśli chodzi o skuteczność, jak i niższe koszty, jeżeli ochrona prywatności jest uwzględniona już od samego początku w fazie projektowania".* Natomiast Giovanni Buttarelli, zastępca EIOD, dodał: „*Ochrona danych jest w pełni kompatybilna z innowacyjnością i nie powinna po prostu być ignorowana w celu utorowania drogi ku krótkoterminowym zyskom. Zasady ochrony prywatności oznaczają, że osoby powinny wiedzieć i być w stanie sprawować kontrolę nad tym, w jakim celu ich dane osobowe będą wykorzystywane, oraz mieć prawo do odwołania się, gdy ich dane są niewłaściwie wykorzystywane lub gdy czują się dyskryminowane"*[432].

Widać tu wyraźnie dbałość o to, aby przed każdym wprowadzeniem nowych przepisów prawa lub rozwiązań technologicznych brana była pod uwagę koncepcja „prywatności w fazie projektowania", lub – jeśli to konieczne – odpowiednia i równoważona ocena wpływu na prywatność, aby potencjalne zagrożenia dla prywatności nie były większe niż rzeczywiste korzyści, które mają wynikać z wprowadzenia nowego przepisu bądź nowej technologii informatycznej.

Rosnące znaczenie ochrony danych we wszystkich obszarach polityki UE oraz szerokie wykorzystywanie technologii informacyjno-komunikacyjnych w praktycznie wszystkich dziedzinach życia i działalności społecznej oznacza, że działalność rzeczników ochrony danych osobowych wykracza poza obszar wolności, bezpieczeństwa i sprawiedliwości oraz

[431] Ochrona prywatności w fazie projektowania (privacy by design) – wbudowanie ochrony danych i prywatności w projekt i architekturę systemów i technologii informacyjno-komunikacyjnych, w celu ułatwienia zapewnienia zgodności z zasadami ochrony danych i prywatności.
[432] www.giodo.gov.pl/plik/id_p/4614/j/pl/

Agendy Cyfrowej UE i obejmuje wiele innych obszarów, m.in. rynek wewnętrzny czy sektor opieki zdrowotnej. W świetle coraz silniejszej tendencji do włączania technologii cyfrowych w różne obszary działalności człowieka, konieczne jest więc określenie jasnych zasad dotyczących wykorzystywania danych osobowych. Jest to szczególnie ważne w odniesieniu do świadczeń usług opieki zdrowotnej z uwagi na podlegający szczególnej ochronie charakter danych dotyczących zdrowia.

Organizacje zainteresowane ochroną praw człowieka, w tym prawa do prywatności i ochrony danych osobowych, z uwagą śledzą badania i raporty dotyczące tego obszaru. Agencja Praw Podstawowych[433] (Fundamental Rights Agency – FRA), unijny organ zajmujący się monitorowaniem przestrzegania praw obywatelskich w Unii Europejskiej, opublikowała raport dotyczący łamania prawa do ochrony danych osobowych. **Badanie FRA** wskazuje, że naruszenia ochrony danych osobowych najczęściej związane są z aktywnością w Internecie, marketingiem bezpośrednim oraz monitoringiem wizyjnym. Podmiotami, na które najczęściej skarżą się obywatele Unii Europejskiej są: administracja publiczna, policja oraz inne służby mundurowe, instytucje finansowe i ochrony zdrowia. Wśród wymienionych szkód związanych z naruszeniem ochrony danych dominują te o charakterze psychologicznym i społecznym – zmniejszenie poczucia bezpieczeństwa, stres, utrata reputacji, niemożność uzyskania kredytu, ograniczony dostęp do opieki zdrowotnej czy świadczeń socjalnych. Publikacja „Access to data protection remedies in the EU Member States" wskazuje też, że ofiary naruszeń prawa do ochrony danych osobowych częściej zgłaszają przypadki naruszeń do organu ds. ochrony danych osobowych niż do sądu. W raporcie tym FRA podkreśla brak odpowiedniego wsparcia prawnego dla ofiar oraz specjalistów w tym zakresie. Adwokaci i sędziowie często nie mają wystarczającej wiedzy na temat ochrony danych, zaś organy ds. ochrony danych są często niedofinansowane i brakuje im specjalistów z dziedziny nowych technologii. W związku z tym FRA zawarła w swej publikacji szereg rekomendacji, podkreślając zwłaszcza konieczność zwiększenia wiedzy o ochronie danych osobowych wśród adwokatów oraz sędziów, a także zapewnienia niezależności organom ochrony danych poprzez zagwarantowanie odpowiednich środków finansowych na ich działalność.

[433] Agencja Praw Podstawowych Unii Europejskiej (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 kolei według danych uzyskanych z **badań przeprowadzonych na potrzeby wspomnianej wcześniej kampanii „Nie daj się okraść. Chroń swoją prywatność**" w ramach Tygodnia Zapobiegania Kradzieży Tożsamości, 60 proc. Polaków nosi w portfelu wszystkie karty kredytowe oraz dokumenty osobiste narażając się na ryzyko jednoczesnej ich utraty. 33 proc. Polaków przyznało się do zagubienia dowodu osobistego, bądź został im on ukradziony, zaś 12 proc. z nas ma zapisany w telefonie komórkowym lub na kartce w portfelu numer PIN karty płatniczej. Świadomość zagrożeń związanych z kradzieżą tożsamości jest bardzo niska w szczególności u osób poniżej 18 roku życia. Stąd ogromne zapotrzebowanie na działania edukacyjne skierowane do najmłodszych użytkowników i potrzeba zintensyfikowania działań GIODO w tym właśnie kierunku.

Podobne wyniki przyniosły **badania Eurobarometru**[434], w którym uczestniczyło 27 tys. osób z państw członkowskich Unii Europejskiej. Badania wykazały, że 76 % europejskich internautów ocenia ryzyko zostania ofiarą cyberprzestępców na coraz większe, zaś 12 % odnotowało atak na swoją elektroniczną skrzynkę pocztową lub konto społecznościowe. Choć 70 % użytkowników sieci w UE jest przeświadczonych, że potrafią robić zakupy czy korzystać z usług banku przez Internet, to w rzeczywistości decyduje się na to tylko 50 % z nich. Dwa najważniejsze obszary obaw co do bezpieczeństwa online, dotyczą nieuczciwego wykorzystywania danych osobowych (co wymienia 37 % badanych) i bezpieczeństwa płatności internetowych (35 %). Natomiast coraz więcej obywateli UE czuje się dobrze poinformowanymi o zagrożeniach w sieci (w 2013 r. - 44 %, w 2012 – 38 %). Nie zawsze jednak wyciągają oni z tej wiedzy właściwe wnioski. Dla przykładu, mniej niż połowa użytkowników zmieniła w ciągu ostatniego roku którekolwiek ze swoich haseł internetowych (w 2013 r. – 48 %, w 2012 r. – 45 %). Znacznie wzrosła też liczba osób korzystających z Internetu za pomocą smartfona (w 2013 r. – 35 %, w 2012 r. – 24 %), bądź tabletu (w 2013 r. – 14 %, w 2012 r. – 6 %)[435]. Badanie wykazało ponadto, że 87 % respondentów

[434] Sondaże Eurobarometru, ośrodka badań opinii publicznej prowadzonych na zlecenie Komisji Europejskiej, przeprowadzane są regularnie we wszystkich państwach Unii Europejskiej, krajach kandydujących, a także na terytorium Cypru Północnego. Ich wyniki publikowane są w postaci ogólnodostępnych raportów. Raporty krajowe powstają dwa razy w roku. Całościowe wyniki badań są dostępne na stronie internetowej: http://ec.europa.eu/public_opinion/archives/flash_arch_en.htm.

[435] Niepokoi również, szczególnie w kontekście wzrostu popularności smartfonów, że w minionym roku 2012 r. jedynie 9% osób ankietowanych na cele raportu Fundacji Bezpieczniej w Sieci, chroniło swoje urządzenia mobilne odpowiednim oprogramowaniem.

unika ujawniania w Internecie osobistych informacji (w 2012 r. – 89 %), zaś 7 % padło ofiarą internetowego oszustwa bankowego lub dotyczącego karty kredytowej.

Zdaniem Cecilii Malmström, Komisarz UE do spraw wewnętrznych, te obawy przekładają się na oszczędne korzystanie z możliwości, jakie daje sieć, co szkodzi zarówno cyfrowej gospodarce, jak i aktywności online. W perspektywie Europejskiej Agendy Cyfrowej, która kładzie nacisk na zaufanie do technologii cyfrowych i bezpieczeństwo, przedstawiona analiza zachowań internautów i użytkowników narzędzi cyfrowych budzi niepokój zarówno ekspertów KE, jak i rzeczników ochrony danych osobowych.

Dlatego szukaniu najlepszych rozwiązań w zakresie ochrony danych osobowych, których wymaga rozwój nowoczesnych technologii, powszechne korzystanie z Internetu i urządzeń mobilnych, a także globalizacja i zawiłość zagadnień związanych z wykorzystywaniem danych osobowych, poświęcone były wszystkie wspomniane w innej części *Sprawozdania* działania edukacyjne GIODO w 2013 r. Generalny Inspektor Ochrony Danych Osobowych zwracał w nich uwagę na coraz bardziej skomplikowane metody przetwarzania informacji, obowiązujące przepisy prawa oraz na kwestie organizacyjne. Dane są wykorzystywane przez międzynarodowe korporacje i przetwarzane w chmurze obliczeniowej, a użytkownicy Internetu korzystają z portali społecznościowych, których serwery znajdują się w różnych państwach, niekiedy niespełniających unijnych standardów bezpieczeństwa danych. To wymaga wspólnych wysiłków, aby świat nie tylko reagował na postęp i rozwój technologiczny, ale także z wyprzedzeniem znajdował rozwiązania, które zapewnią odpowiednią ochronę przetwarzanych informacji. We współczesnym świecie korzystanie na masową skalę z internetowych interfejsów i aplikacji, zwłaszcza tych mobilnych, jest **największym wyzwaniem dla ochrony prywatności.** Przy czym nie chodzi tu o to, by powstrzymać rozwój nowoczesnych technologii, ale by „cywilizować sposób ich używania". Mobilne aplikacje – rozsyłające informacje o naszych poczynaniach – często instalujemy sami, zwłaszcza, gdy są one bezpłatne. Konfigurujemy je z innymi urządzeniami mobilnymi, jak laptopy, tablety czy komputery pokładowe w samochodzie, otwierając dostęp do ich zawartości. Generalny Inspektor Ochrony Danych Osobowych nieustannie podkreśla, że nawet wyrażając zgodę na działanie aplikacji, nie jesteśmy do końca świadomi tego, na co się tak naprawdę zgodziliśmy. A wtedy trudno jest stwierdzić, że jest to zgoda „dobrze poinformowanej osoby". Dlatego różne raporty na temat aplikacji mobilnych publikowane

przez środowisko ochrony danych w ubiegłych latach[436], zawierają cenne wytyczne dotyczące relacji między aplikacjami a ochroną prywatności. Wśród nich wymienić należy wspomnianą wcześniej **Deklarację Warszawską w sprawie upowszechniania się aplikacji w społeczeństwie** przyjętą podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności zorganizowanej przez GIODO we wrześniu 2013 r. w Warszawie. W opinii Generalnego Inspektora Ochrony Danych Osobowych ważne jest również doprecyzowanie znaczenia pojęcia „prywatność" w europejskim znaczeniu tego terminu, do czego konieczny jest międzynarodowy dialog i wspólne działania na rzecz wprowadzenia regulacji i jednolitych standardów ochrony danych osobowych. To, co różni kraje pomiędzy sobą, to świadomość konsumentów na temat tego, co dzieje się z ich danymi osobowymi oraz przyjęte w danym kraju rozwiązania prawne. Dlatego przed rzecznikami ochrony danych stoi ważne zadanie – budowanie takich rozwiązań chroniących dane osobowe obywateli, aby od początku były one dostosowane do ochrony tego podstawowego prawa obywateli.

W podsumowaniu podkreślenia wymaga, że polskie prawo trzeba dobrze przygotować do radzenia sobie ze współczesnymi wyzwaniami. Ustawa o ochronie danych osobowych powstała w 1997 r. w oparciu o unijną dyrektywę z 1995 r., a od tego czasu uchwalono 18 zmieniających tę ustawę aktów prawnych. Pamiętać też trzeba, że ochrona danych osobowych dotyczy bardzo wielu obszarów prawa i problemy pojawiają się nie tylko np. w kontekście wprowadzania systemów informacji medycznej czy informacji oświatowej, ale także w sferze prawa transportowego, bankowego czy ubezpieczeniowego. Dlatego nowelizacja jest potrzebna, bo pomimo przestarzałych przepisów świadomość Polaków dotycząca ochrony danych osobowych wciąż rośnie, o czym świadczy liczba kilku tysięcy spraw, które co roku wpływają do Biura GIODO rozpoczynając postępowanie administracyjne i tyle samo pytań o interpretację aktów prawnych związanych z ochroną danych osobowych.

[436] *Opinia w sprawie aplikacji w urządzeniach mobilnych* Grupy Roboczej Artykułu 29 ds. Ochrony Danych Unii Europejskiej, *Wytyczne dla twórców aplikacji* Rzecznika Ochrony Prywatności Kanady, raport pracowników Federalnej Komisji Handlu *Ujawnianie prywatności w urządzeniach mobilnych: budowanie zaufania poprzez przejrzystość* oraz *Memorandum Sopockie* Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji.

ZAŁĄCZNIKI:

Załącznik nr 1

Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2013 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego

L.p.	Nazwa podmiotu, do którego skierowano wystąpienie	Data wystąpienia/ Sygnatura sprawy	Przedmiot wystąpienia
1.	Minister Nauki i Szkolnictwa Wyższego	28.01.2013 DIS-K-421/144/12	Podjęcie prac legislacyjnych mających na celu doprecyzowanie zakresu danych osobowych przetwarzanych w Systemie Informacji o Szkolnictwie Wyższym.
2.	Dyrektor Instytutu Hematologii i Transfuzjologii w Warszawie	18.02.2013 DIS-K-421/93,96,97, 109/12	Zmodyfikowanie formularza o nazwie „Karta Ewidencyjna Ogólnopolskiego Centralnego Rejestru Dawców Szpiku i Krwi Pępowinowej", aby spełniał wymogi ustawy o ochronie danych osobowych.
3.	Minister Sprawiedliwości	8.03.2013 DOLiS-035-110/13	Konieczność respektowania prawa do prywatności oraz ochrony informacji dotyczących osób obsługiwanych w punktach obsługi interesantów w sądach powszechnych.
4.	Minister Spraw Wewnętrznych	15.03. 2013 DOLiS-035-553/13	Podjęcie prac legislacyjnych zmierzających do zmiany przepisów Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 22 czerwca 2011 r. w sprawie usuwania pojazdów pozostawionych bez tablic rejestracyjnych lub których stan wskazuje na to, że nie są używane (Dz. U. z 2011 r., Nr 143, poz. 845 z późn. zm.) w zakresie udostępnienia danych osobowych właścicieli pojazdów, w celu usprawnienia działań podmiotów publicznych uczestniczących w działaniach określonych jego przepisami.
5.	Szef Służby Celnej	08.04.2013 DIS-K-421/13,15,16/13	Podjęcie działań, które zapewnią, że realizacja przedsięwzięć wspierających pracę Służby Celnej, które wiążą się z przetwarzaniem danych osobowych, będzie następowała z zachowaniem wymogów wynikających z przepisów o ochronie danych osobowych.
6.	Minister Administracji i Cyfryzacji	27.05.2013 DOLiS-072-12/13	Wystąpienie do Ministerstwa Administracji i Cyfryzacji w sprawie wzorów deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi kształtujących zakres danych osobowych pozyskiwanych od mieszkańców gminy.
7.	Dyrektor Generalny Polskiej Izby Hotelarstwa	26.06.2013 DOLiS-035-1621/13	Zapewnienie prawidłowości procesu przetwarzania danych przechowywanych przez placówki hotelarskie.

8.	Minister Pracy i Polityki Społecznej	29.07.2013 DOLiS-035-1996/13	Wystąpienie do Ministra Pracy i Polityki Społecznej o rozważenie wprowadzenia w przepisach ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej (t.j. Dz.U.2013.135) zmian w zakresie regulacji dotyczących przetwarzania danych osobowych.
9.	Minister Transportu, Budownictwa i Gospodarki Morskiej	31.07. 2013 DOLiS-035-1996/13	Wystąpienie do Ministra Transportu, Budownictwa i Gospodarki Morskiej z prośbą o podjęcie prac legislacyjnych mających na celu kompleksowe uregulowanie problematyki dot. przetwarzania danych przez starostów, którzy dokonują rejestracji pojazdu.
10.	Rada Miejska w Łodzi	08.08.2013 DIS-K-421/66/13	Podjęcie działań mających na celu zmianę wzorów deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzorów deklaracji z przepisami ochronie danych osobowych.
11.	Rada Miejska Nowe Brzesko	14.08.2013 DIS-K-421/78/13	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami ochronie danych osobowych.
12.	Areszt Śledczy	3.09.2013 DOLiS-035-2172-13	Wystąpienie do jednego z aresztów śledczych o podjęcie działań mających na celu dostosowanie procesu przetwarzania przez Areszt Śledczy danych osobowych osób w nim osadzonych do wymogów określonych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
13.	Zakład Karny	3.09.2013 DOLiS-2245/13	Wystąpienie o podjęcie działań mających na celu dostosowanie procesu przechowywania i przetwarzania przez Zakład Karny danych osobowych osób w nim osadzonych do wymogów określonych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
14.	Naczelna Rada Lekarska	19.09.2013 DIS-K-421/169/12	Prośba o zbadanie sprawy przez organy samorządu zawodowego lekarzy w ramach sprawowanego nadzoru nad wykonywaniem zawodu lekarza.
15.	Prezydent m.st. Warszawy	24.09.2013 DIS-K-421/61 i 62/13	Podjęcie działań zmierzających do ujednolicenia zasad stosowania oświadczeń dotyczących podstaw prawnych przetwarzania danych osobowych dzieci i ich rodziców/opiekunów prawnych w przedszkolach prowadzonych przez Miasto Stołeczne Warszawa.
16.	Rada Miejska w Krzeszowicach	08.10.2013 DIS-K-421/111/13	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami ochronie danych osobowych.
17.	Rada Miejska w Piastowie	16.10.2013 DIS-K-421/58/13	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami ochronie danych osobowych.
18.	Prokurator Generalny	21.10.2013 DIS-K-421/132/12 i 37/13	Udzielenie informacji o sposobie, w jaki jeden z operatorów telekomunikacyjnych będzie udostępniał dane telekomunikacyjne Prokuraturze

			Generalnej i jej jednostkom organizacyjnym, w okresie po rozwiązaniu porozumienia zawartego pomiędzy tym operatorem telekomunikacyjnym a Prokuraturą Generalną.
19.	Wojewoda Łódzki	21.10.2013 DIS-K-421/66/13	Podjęcie działań mających na celu zapewnienie zgodności z przepisami ochronie danych osobowych uchwały określającej wzór deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi.
20.	Rada Miejska Częstochowy	30.10.2013 DIS-K-421/74/13	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami ochronie danych osobowych.
21.	Rada m.st. Warszawy	13.11.2013 DIS-K-421/69, 83 i 94/13	Podjęcie działań mających na celu zmianę wzorów deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzorów deklaracji z przepisami ochronie danych osobowych.
22.	Minister Edukacji Narodowej	6.11. 2012 DOLiS-035-3533/13	Wystąpienie w związku z udostępnieniem na stronie internetowej Ministerstwa Edukacji Narodowej danych osobowych ekspertów MEN, które w opinii GIODO nastąpiło bez podstawy prawnej.
23.	Minister Sprawiedliwości	6.11.2013 DOLiS-035-3530-13	Wystąpienie o podjęcie prac legislacyjnych mających na celu doprecyzowanie § 8 ust. 1 rozporządzenia Ministra Sprawiedliwości z dnia 24 stycznia 2005 r. w sprawie biegłych sądowych (Dz. U. z Nr 15 poz. 133) poprzez określenie rodzaju adresu biegłego sądowego zamieszczanego w wykazach i listach prowadzonych przez prezesów sądów, w sposób uniemożliwiający podawanie do publicznej wiadomości informacji obejmujących prywatną sferę życia biegłego sądowego.
24.	Samorządowe Kolegium Odwoławcze	20.11.2013 DOLiS-035-3675/13	Wystąpienie w sprawie informacji o stosowaniu przez Samorządowe Kolegium Odwoławcze formularza wniosku o udostępnienie informacji publicznej, w którym wymagane jest podanie adresu, numeru PESEL i numeru telefonu wnioskodawcy, pomimo, iż wnioskodawca ma możliwość otrzymania odpowiedzi na adres poczty elektronicznej, oraz udzielanie zgody na przetwarzanie danych w celu realizacji przedmiotowego wniosku.
25.	Uczelnia Wyższa	13.12.2013 DOLiS-035-3568/13	Wystąpienie do jednej z uczelni wyższej o podjęcie stosownych działań w celu wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych osób, które odwiedzają studenta w akademiku.
26.	Komendant Główny Policji	20.12.2013 DOLiS-035-4126-13	Wystąpienie o podjęcie działań mających na celu zaznajomienie funkcjonariuszy Policji z podstawowymi zagadnieniami dotyczącymi ochrony danych osobowych, w szczególności kwestii związanych z pozyskiwaniem danych osobowych oraz przepisów karnych ustawy z dnia

			29 sierpnia 1997 roku o ochronie danych osobowych, w tym uwrażliwienie funkcjonariuszy Policji na fakt, że do Generalnego Inspektora Ochrony Danych Osobowych nie należy kierować wniosków o udostępnienie danych osobowych, gdyż stosownie do art. 12 ustawy o ochronie danych osobowych udostępnianie takich danych pozostaje poza zakresem kompetencji organu.

Załącznik nr 2

Wykaz kontroli przeprowadzonych w 2013 r.

L.p.	Data / Sygnatura kontroli	Nazwa podmiotu i miejsce kontroli	Inicjatywa kontroli	Rozstrzygnięcie
1.	07-11.01.2013 DIS-K-421/1/13	Zarząd Dróg Miejskich, Warszawa, ul. Chmielna 120	z urzędu	decyzja GIODO
2.	14-17.01.2013 DIS-K-421/2/13	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
3.	14-17.01.2013 DIS-K-421/3/13	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
4.	14-18.01.2013 DIS-K-421/4/13	Centrum Rozwoju Zasobów Ludzkich, Warszawa, Al. Jerozolimskie 65/79	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
5.	14-18.01.2013 DIS-K-421/5/13	Online Media Group Poland Sp. z o.o., Warszawa, Al. Jerozolimskie 107	w związku z kontrolą DIS-K-421/146/12	nie stwierdzono uchybień
6.	21-25.01.2013 DIS-K-421/6/13	EURO-KONSULT Sp. z o.o. Lublin, ul. Narutowicza 57/8	w związku z kontrolą DIS-K-421/54/12	nie stwierdzono uchybień
7.	21-25.01.2013 DIS-K-421/7/13	Evolution Media Net Sp. z o.o., Warszawa, ul. Wilcza 46	w związku z kontrolą DIS-K-421/146/12	brak przetwarzania danych osobowych w zakresie objętym kontrolą
8.	21-25.01.2013 DIS-K-421/8/13	Auchan Polska Sp. z o.o. Piaseczno, ul. Puławska 46	z urzędu	decyzja GIODO
9.	24-25.01.2013 DIS-K-421/9/13	P4 Sp. z o.o., Warszawa, ul. Taśmowa 7	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
10.	28-29.01.2013 DIS-K-421/10/13	Wspólnota Mieszkaniowa „Wileńska 18”, Warszawa, ul. Wileńska 18	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
11.	28.01.-01.02.2013 DIS-K-421/11/13	Generali Towarzystwo Ubezpieczeń S.A., Warszawa, ul. Postępu 15B	z urzędu	decyzja GIODO
12.	28.01.-01.02.2013 DIS-K-421/12/13	Netia S.A., Warszawa, ul. Poleczki 13	z urzędu	decyzja GIODO
13.	04-08.02.2013 DIS-K-421/13/13	Ministerstwo Finansów Departament Służby Celnej, Warszawa, ul. Świętokrzyska 12	Departament Edukacji Społecznej i Współpracy Międzynarodowej	zaprzestano przetwarzania danych osobowych
14.	06-08.02.2013 DIS-K-421/14/13	Go Sport Polska Sp. z o.o. Warszawa, ul. Ostrobramska 75B	Departament Orzecznictwa Legislacji i Skarg	brak przetwarzania danych osobowych w zakresie objętym kontrolą
15.	06-08.02.2013 DIS-K-421/15/13	Urząd Celny III „Port Lotniczy” w Warszawie, Warszawa, ul. Żwirki i Wigury 1	Departament Edukacji Społecznej i Współpracy Międzynarodowej	zaprzestano przetwarzania danych osobowych
16.	06-08.02.2013	Izba Celna w Warszawie,	Departament	zaprzestano przetwarzania danych

	DIS-K-421/16/13	Warszawa, ul. Ciołka 14A	Edukacji Społecznej i Współpracy Międzynarodowej	osobowych
17.	11-15.02.2013 DIS-K-421/17/13	Getin Noble Bank S.A., Warszawa, ul. Domaniewska 39	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
18.	11-14.02.2013 DIS-K-421/18/13	Inter Ikea Centre Polska S.A., Janki, Pl. Szwedzki 3	z urzędu	przywrócono stan zgodny z prawem
19.	11-15.02.2013 DIS-K-421/19/13	Jeronimo Martins Polska S.A., Warszawa, ul. Dolna 3	z urzędu	przywrócono stan zgodny z prawem
20.	18-22.02.2013 DIS-K-421/20/13	Zarząd Dróg i Transportu, Łódź, ul. Piotrkowska 175	z urzędu	nie stwierdzono uchybień
21.	25.02.-01.03.2013 DIS-K-421/21/13	Komendant Główny Straży Granicznej – Placówka Straży Granicznej Warszawa – Okęcie, Warszawa, ul. 17 stycznia 45D	z urzędu	nie stwierdzono uchybień
22.	25.02.-01.03.2013 DIS-K-421/22/13	Tesco (Polska) Sp. z o.o. Kraków, ul. Kapelanka 56	z urzędu	decyzja GIODO
23.	25.02.-01.03.2013 DIS-K-421/23/13	Prezydent Miasta Gdańska – Urząd Miejski w Gdańsku, Gdańsk, ul. Nowe Ogrody 8/12	z urzędu	nie stwierdzono uchybień
24.	26-27.02. 2013 DIS-K-421/24/13	Uniwersytecka Szkoła Kształcenia Indywidualnego Sp. z o.o., Kraków, ul. Ładna 2	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
25.	04-08.03.2013 DIS-K-421/25/13	Shell Polska Sp. z o.o., Warszawa, ul. Bitwy Warszawskiej 1920 r. 7A	z urzędu	decyzja GIODO
26.	04-08.03.2013 DIS-K-421/26/13	Zarząd Dróg i Mostów, Lublin, ul. Krochmalna 13	z urzędu	nie stwierdzono uchybień
27.	11-15.03.2013 DIS-K-421/27/13	Szef Służby Celnej, Warszawa, ul. Świętokrzyska 12	z urzędu	przywrócono stan zgodny z prawem
28.	11-15.03.2013 DIS-K-421/28/13	Generalny Inspektor Kontroli Skarbowej, Warszawa, ul. Świętokrzyska 12	z urzędu	decyzja GIODO
29.	13-15.03.2013 DIS-K-421/29/13	Adam Gumkowski prowadzący działalność gospodarczą pod nazwą „AG Klinik Adam Gumkowski”, Warszawa, ul. Kazimierzowska 43	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
30.	18-21.03.2013 DIS-K-421/30/13	Sephora Polska Sp. z o.o. Warszawa, Al. Jerozolimskie 92	z urzędu	decyzja GIODO
31.	18-22.03.2013 DIS-K-421/31/13	Peek & Cloppenburg Sp. z o.o., Warszawa, Al. Jana Pawła II 61 lok. 248	z urzędu	decyzja GIODO
32.	18-21.03.2013 DIS-K-421/32/13	Statoil Fuel & Retail Polska Sp. z o.o. Warszawa, ul. Puławska 86	z urzędu	decyzja GIODO
33.	18-22.03.2013 DIS-K-421/33/13	Europejskie Centrum Odszkodowawcze S.A., Legnica, ul. Kolbego 18	Prokuratura Apelacyjna w Rzeszowie	decyzja GIODO
34.	20-26.03.2013 DIS-K-421/34/13	Centralny Organ Techniczny KSI (Komendant Główny Policji), Warszawa, ul. Puławska 148/150	z urzędu	zalecenia pokontrolne
35.	25-29.03.2013 DIS-K-421/35/13	Urząd Skarbowy w Sosnowcu, Sosnowiec, ul. 3 Maja 20	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO

36.	25-28.03.2013 DIS-K-421/36/13	KoppAhl Polska Sp. z o.o. Warszawa, ul. Leszno 12	z urzędu	decyzja GIODO
37.	25-27.03.2013 DIS-K-421/37/13	Prokuratura Okręgowa w Warszawie, Warszawa, ul. Chocimska 28	z urzędu	wystąpienie do Prokuratora Generalnego
38.	08-12.04.2013 DIS-K-421/38/13	Spółdzielnia Mieszkaniowa „Pojezierze", Olsztyn, ul. Kołobrzeska 13	Prokuratura Rejonowa Olsztyn - Południe	nie stwierdzono uchybień
39.	08-12.04.2013 DIS-K-421/39/13	Uniwersytet Medyczny im. Karola Marcinkowskiego, Poznań, ul. Fredry 10	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
40.	09-12.04.2013 DIS-K-421/40/13	Wojewódzki Ośrodek Ruchu Drogowego w Warszawie, Warszawa, ul. Odlewnicza 8	Rzecznik Praw Obywatelskich	decyzja GIODO
41.	15-17.04.2013 DIS-K-421/42/13	Sebastian Serek prowadzący działalność gospodarczą pod nazwą „P.U.H. Rozwój Sebastian Serek", Poznań, ul. Kwiatowa 14	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
42.	15-16.04.2013 DIS-K-421/43/13	Jerzy Kański prowadzący działalność gospodarczą pod nazwą „HALL CARS 2 Jerzy Kański", Łódź, ul. Pabianicka 245	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
43.	15-18.04.2013 DIS-K-421/44/13	Katarzyna Króliszyn prowadząca działalność gospodarczą pod nazwą „Wonder World Katarzyna Króliszyn", Łódź, ul. Tuszyńska 139/143 lok. 15	z urzędu	nie stwierdzono uchybień
44.	15-19.04.2013 DIS-K-421/45/13	Bank Millennium S.A., Warszawa, ul. St. Żaryna 2A	z urzędu	nie stwierdzono uchybień
45.	22-26.04.2013 DIS-K-421/46/13	Iwona Mirońska prowadząca działalność gospodarczą pod nazwą „Przedsiębiorstwo Handlowo – Usługowe Medi – Soft Punkt Apteczny Iwona Mirońska", Serock, ul. Nasielska 19A	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
46.	22-26.04.2013 DIS-K-421/47/13	Narodowy Fundusz Zdrowia, Warszawa, ul. Grójecka 186	Departament Rejestracji Zbiorów Danych Osobowych	nie stwierdzono uchybień
47.	22-26 i 29- 30.04.2013 DIS-K-421/48/13	Generalny Dyrektor Dróg Krajowych i Autostrad, Warszawa, ul. Wronia 63	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
48.	22-26 i 29- 30.04.2013 DIS-K-421/49/13	Kapsch Telematic Services Sp. z o.o., Warszawa, ul. Poleczki 35	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
49.	07-10.05.2013 DIS-K-421/50/13	Polska Agencja Rozwoju Przedsiębiorczości, Warszawa, ul. Pańska 81/83	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
50.	07-10.05.2013 DIS-K-421/51/13	Ministerstwo Rozwoju Regionalnego, Warszawa, ul. Wspólna 2/4	w związku z kontrolą DIS-K- 421/4/13	usunięto uchybienia
51.	08-10.05.2013 DIS-K-421/52/13	Polanowscy Nieruchomości Sp. z o.o., Warszawa, ul. Marszałkowska 83	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg

52.	13-16.05.2013 DIS-K-421/53/13	Lechia Gdańsk S.A., Gdańsk, ul. Pokoleń Lechii Gdańsk 1	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
53.	13-16.05.2013 DIS-K-421/54/13	Lechia Gdańsk S.A., Gdańsk, ul. Pokoleń Lechii Gdańsk 1	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
54.	13-17.05.2013 DIS-K-421/55/13	Wojewódzki Szpital dla Nerwowo i Psychicznie Chorych „Drewnica" SP ZOZ, Ząbki, ul. Rychlińskiego 1	z urzędu	decyzja GIODO
55.	13-17.05.2013 DIS-K-421/56/13	Instytut Psychiatrii i Neurologii, Warszawa, ul. Sobieskiego 9	z urzędu	nie stwierdzono uchybień
56.	13-17. i 22-24.05.2013 DIS-K-421/57/13	Powszechna Kasa Oszczędności Bank Polski S.A. I Oddział w Zduńskiej Woli, Zduńska Wola, ul. Łaska 46	Prokuratura Rejonowa w Zduńskiej Woli	nie stwierdzono uchybień
57.	20-24.05.2013 DIS-K-421/58/13	Urząd Miejski w Piastowie, Piastów, ul. 11 Listopada 2	Zespół Prasowy	wystąpienie do Rady Miejskiej w Piastowie
58.	20-24.05.2013 DIS-K-421/59/13	Ebitda Sp. z o.o., Poznań, ul. Szarych Szeregów 27	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
59.	20-24.05.2013 DIS-K-421/60/13	Drugi Urząd Skarbowy w Rzeszowie, Rzeszów, ul. Siemieńskiego 18	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
60.	20-21.05.2013 DIS-K-421/61/13	Przedszkole nr 44, Warszawa, ul. Ludna 8	Rzecznik Praw Obywatelskich	nie stwierdzono uchybień
61.	20-23.05.2013 DIS-K-421/62/13	Przedszkole Integracyjne nr 17 „Przyjazna Kraina", Warszawa, ul. Sielecka 26	Rzecznik Praw Obywatelskich	nie stwierdzono uchybień
62.	05-07.06.2013 DIS-K-421/64/13	Business Zone Sp. z o.o., Warszawa, ul. Chałubińskiego 8	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
63.	05-06.06.2013 DIS-K-421/65/13	Celier Aviation Sp. z o.o., Warszawa, ul. Fabryczna 16 lok. 22,	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
64.	10-14.06.2013 DIS-K-421/66/13	Prezydent Miasta Łodzi – Urząd Miasta Łodzi, Łódź, ul. Piotrkowska 104	z urzędu	decyzja GIODO wystąpienie do Wojewody Łódzkiego
65.	10-14.06.2013 DIS-K-421/67/13	Główny Inspektor Transportu Drogowego, Warszawa, ul. Postępu 21	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
66.	10-14.06.2013 DIS-K-421/68/13	Bank BPH S.A., Gdańsk, ul. Marynarki Polskiej 177,	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
67.	10-14.06.2013 DIS-K-421/69/13	Prezydent m.st. Warszawy – Urząd m.st. Warszawy, Warszawa, Pl. Bankowy 3/5	z urzędu	wystąpienie do Rady m.st. Warszawy
68.	17-19.06.2013 DIS-K-421/70/13	Niezależny Operator Międzystrefowy Sp. z o.o., Warszawa,ul. Murmańska 25	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
69.	18-21.06.2013 DIS-K-421/71/13	Western Union Payment Services Ireland Limited Oddział w Polsce, Warszawa, Al. Jana Pawła 29	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
70.	18-20.06.2013 DIS-K-21/72/13	Free4Fresh Sp. z o.o. Warszawa, ul. Jutrzenki 177	z urzędu	nie stwierdzono uchybień
71.	19-21.06.2013 DIS-K-421/73/13	Piano Media Sp. z o.o. Warszawa, ul. Sienna 72/6	z urzędu	nie stwierdzono uchybień

72.	24-28.06.2013 DIS-K-421/74/13	Urząd Miasta Częstochowy, Częstochowa, ul. Śląska 11/13	z urzędu	wystąpienie do Rady Miasta Częstochowy
73.	26-28.06.2013 DIS-K-421/75/13	Spotify Poland Sp. z o.o. Warszawa, Pl. Piłsudskiego 1	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
74.	25-27.06.2013 DIS-K-421/76/13	Spółdzielnia Mieszkaniowa Wola, Warszawa, ul. Powstańców Śląskich 104	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
75.	24-28.06.2013 DIS-K-421/77/13	Euro Net Sp. z o.o. Warszawa, ul. Muszkieterów 15	z urzędu	decyzja GIODO
76.	01-05.07.2013 DIS-K-421/78/13	Burmistrz Gminy i Miasta Nowe Brzesko, Nowe Brzesko, ul. Krakowska 44	z urzędu	decyzja GIODO wystąpienie do Rady Miejskiej Nowe Brzesko
77.	01-05.07.2013 DIS-K-421/79/13	Prezydent Miasta Lublina, Lublin, Pl. Króla Wł. Łokietka 1	z urzędu	wystąpienie do Rady Miasta Lublin
78.	02-03.07.2013 DIS-K-421/80/13	Intrum Justitia Sp. z o.o. Warszawa, ul. Domaniewska 41	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
79.	02.07.2013 DIS-K-421/81/13	Urząd do Spraw Cudzoziemców, Warszawa, ul. Koszykowa 16	z urzędu	nie stwierdzono uchybień
80.	08-10.07.2013 DIS-K-421/82/13	Pomocna Pożyczka Sp. z o.o. Gdańsk, ul. Saperów 19	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
81.	08-11.07.2013 DIS-K-421/83/13	Prezydent m.st. Warszawy – Urząd Dzielnicy Bemowo m.st. Warszawy, Warszawa, ul. Powstańców Śląskich 70	z urzędu	nie stwierdzono uchybień
82.	08-12.07.2013 DIS-K-421/84/13	Frisco.pl Sp. z o.o. Warszawa, ul. Omulewska 27	z urzędu	decyzja GIODO
83.	08-12.07.2013 DIS-K-421/85/13	Michał Bachewicz prowadzący działalność gospodarczą pod nazwą „Sklep komputerowy Bachcomp Michał Bachewicz”, Toruń, ul. Staszica 8A	z urzędu	decyzja GIODO
84.	15-19.07.2013 DIS-K-421/86/13	Adam Mendelka prowadzący działalność gospodarczą pod nazwą „Adam Mendelka ADEX”, Warszawa, ul. Bychowska 59A/2	z urzędu	decyzja GIODO
85.	15-19.07.2013 DIS-K-421/87/13	Urząd Gminy Komorniki Komorniki, ul. Stawna 1	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
86.	15-19.07.2013 DIS-K-421/88/13	Włodzimierz Lapis prowadzący działalność gospodarczą pod nazwą „Centrum Oświatowo – Wydawnicze Promotor”, Komorniki, ul. Morenowa 16	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
87.	16-19.07.2013 DIS-K-421/89/13	Agito S.A., Warszawa, ul. Mokotowska 1	z urzędu	decyzja GIODO
88.	15-19.07.2013 DIS-K-421/90/13	PTS S.A., Wrocław, ul. Szewska 5	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
89.	15-19.07.2013 DIS-K-421/91/13	PTS S.A., Wrocław, ul. Szewska 5	Departament Orzecznictwa	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg

			Legislacji i Skarg	
90.	15-19.07.2013 DIS-K-421/92/13	PTS S.A., Wrocław, ul. Szewska 5	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
91.	22-25.07.2013 DIS-K-421/93/13	Instytut Szkoleń Profesjonalnych Sp. z o.o., Gdańsk, ul. Wałowa 17 lok. 209	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
92.	22-25.07.2013 DIS-K-421/94/13	Urząd Dzielnicy Mokotów m.st. Warszawy, Warszawa, ul. Rakowiecka 25/27	z urzędu	wystąpienie do Rady m.st. Warszawy
93.	22-26.07.2013 DIS-K-421/95/13	Medtronic Poland Sp. z o.o., Warszawa, ul. Ostobramska 101	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
94.	29.07.-01.08.2013 DIS-K-421/97/13	Urząd Kontroli Skarbowej, Warszawa, ul. Cybernetyki 19B	z urzędu	nie stwierdzono uchybień
95.	01-02.08.2013 DIS-K-421/98/13	Urząd m.st. Warszawy, Warszawa, Pl. Bankowy 3/5	w związku z kontrolą DIS-K-421/1/13	decyzja GIODO
96.	06-09.08.2013 DIS-K-421/99/13	Publicze Sp. z o.o., Warszawa, ul. Vogla 2A	z urzędu	decyzja GIODO
97.	05-09.08.2013 DIS-K-421/100/13	Komenda Główna Policji, Warszawa, ul. Puławska 148/150	Najwyższa Izba Kontroli	pismo do Komendanta Głównego Policji
98.	05-09.08.2013 DIS-K-421/101/13	NET-S M. Chmielewski sp.j., Gdynia, ul. Starowiejska 17	z urzędu	decyzja GIODO
99.	19-23.08.2013 DIS-K-421/102/13	Komenda Wojewódzka Policji w Lublinie, Lublin, ul. Narutowicza 73	Najwyższa Izba Kontroli	pismo do Komendanta Głównego Policji
100.	19-23.08.2013 DIS-K-421/103/13	Komenda Miejska Policji w Lublinie, Lublin, ul. Północna 3	Najwyższa Izba Kontroli	pismo do Komendanta Głównego Policji
101.	19 i 21.08.2013 DIS-K-421/104/13	Urząd Celny w Toruniu, Toruń, ul. Batorego 61	z urzędu	nie stwierdzono uchybień
102.	19-23.08.2013 DIS-K-421/105/13	Izba Celna w Toruniu, Toruń, ul. Mazowiecka 63/65	z urzędu	nie stwierdzono uchybień
103.	26-30.08.2013 DIS-K-421/107/13	Komenda Wojewódzka Policji w Kielcach, Kielce, ul. Seminaryjska 12	Najwyższa Izba Kontroli	nie stwierdzono uchybień
104.	26-30.08.2013 DIS-K-421/108/13	Komenda Miejska Policji w Kielcach, Kielce, ul. Wesoła 43	Najwyższa Izba Kontroli	nie stwierdzono uchybień
105.	26-30.08.2013 DIS-K-421/109/13	Polska Agencja Rozwoju Przedsiębiorczości, Warszawa, ul. Pańska 81/83	w związku z kontrolą DIS-K-421/50/13	decyzja GIODO
106.	28-30.08.2013 DIS-K-421/110/13	Telekomunikacja Polska S.A., Warszawa, ul. Twarda 18	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
107.	02-06.09.2013 DIS-K-421/111/13	Urząd Miejski Krzeszowice, Krzeszowice, ul. Ogrodowa 1	z urzędu	decyzja GIODO wystąpienie do Rady Miasta Krzeszowice
108.	02-06.09.2013 DIS-K-421/112/13	Narodowy Fundusz Zdrowia, Warszawa, ul. Grójecka 186	Departament Rejestracji Zbiorów Danych Osobowych	przywrócono stan zgodny z prawem
109.	03-05.09.2013 DIS-K-421/113/13	Vectra S.A., Gdynia, Al. Zwycięstwa 253	Zespół ds. Naruszeń Danych Osobowych	wnioski przekazano do Zespołu ds. Naruszeń Danych Osobowych
110.	03-06.09.2013	Netia S.A., Warszawa,	Zespół ds. Naruszeń	decyzja GIODO

	DIS-K-421/114/13	ul. Poleczki 13	Danych Osobowych	
111.	03.09.2013 DIS-K-421/115/13	Jacek Powsiński, Warszawa, ul. Wilcza 8 lok. 3	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
112.	09-11.09.2013 DIS-K-421/116/13	Urząd Skarbowy Warszawa - Wawer, Warszawa, ul. Mycielskiego 21	w związku z kontrolą DIS-K-421/93/13	nie stwierdzono uchybień
113.	09-11.09.2013 DIS-K-421/117/13	Urząd Skarbowy Warszawa - Bemowo, Warszawa, ul. Białobrzeska 53a	w związku z kontrolą DIS-K-421/93/13	nie stwierdzono uchybień
114.	09-11.09.2013 DIS-K-421/118/13	Urząd Skarbowy Warszawa - Praga, Warszawa, ul. Jagiellońska 15	w związku z kontrolą DIS-K-421/93/13	nie stwierdzono uchybień
115.	09-13.09.2013 DIS-K-421/119/13	Straż Gminna Gminy Słupsk, Słupsk, ul. Kolejowa 5a	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
116.	09-13.09.2013 DIS-K-421/120/13	Straż Gminna Gminy Słupsk, Słupsk, ul. Kolejowa 5a	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
117.	09-13.09.2013 DIS-K-421/121/13	Urząd Miasta Bolesławiec, Bolesławiec, ul. Rynek 41	z urzędu	nie stwierdzono uchybień
118.	16-18.09.2013 DIS-K-421/123/13	Pierwszy Urząd Skarbowy w Lublinie, Lublin, ul. Sądowa 5	z urzędu	nie stwierdzono uchybień
119.	19-20.09.2013 DIS-K-421/124/13	Bartosz Bąk prowadzący działalność gospodarczą pod nazwą „szybkopewnie.pl Bartosz Bąk”, Lublin, ul. Zana 10/63	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
120.	16-20.09.2013 DIS-K-421/125/13	Komandos Łódź Sp. z o.o., Łódź, ul. Brzeźna 3	Prokuratura Rejonowa w Pabianicach	decyzja GIODO
121.	16-20. i 22-26.09.2013 DIS-K-421/126/13	Urząd do Spraw Cudzoziemców, Warszawa, ul. Koszykowa 16	z urzędu	decyzja GIODO
122.	23-27.09.2013 DIS-K-421/127/13	Erasmus Sp. z o.o., Olsztyn, ul. Dworcowa 3/104	Rzecznik Praw Obywatelskich	nie stwierdzono uchybień
123.	23-25.09.2013 DIS-K-421/128/13	Tomasz Sobecki prowadzący działalność gospodarczą pod nazwą „TS research Tomasz Sobecki”, Warszawa, ul. Picassa 5/14	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
124.	23-27.09.2013 DIS-K-421/129/13	Topmarket Sp. z o.o., Warszawa, ul. Instalatorów 7B	z urzędu	nie stwierdzono uchybień
125.	23-25.09.2013 DIS-K-421/130/13	Krajowy Rejestr Usług Sp. z o.o., Wrocław, ul. Pilczycka 201	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
126.	23-25.09.2013 DIS-K-421/131/13	Krajowy Rejestr Usług Sp. z o.o., Wrocław, ul. Pilczycka 201	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
127.	23-25.09.2013 DIS-K-421/132/13	Lexis Polska Sp. z o.o., Wrocław, ul. Pilczycka 201	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
128.	23-25.09.2013 DIS-K-421/133/13	Lexis Polska Sp. z o.o., Wrocław, ul. Pilczycka 201	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
129.	01-04.10.2013	Krajowy Rejestr Pracowników i	w związku z	ustalenia z kontroli wykorzystano

	DIS-K-421/134/13	Pracodawców Sp. z o.o., Grudziądz, ul. Mickiewicza 51-53	kontrolą DIS-K-421/87/12	w postępowaniu DIS-K-421/87/12
130.	01-04.10.2013 DIS-K-421/135/13	Fundacja na Rzecz Chorych z Chorobami Krwi, Warszawa, ul. Bagatela 14	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
131.	07-11.10.2013 DIS-K-421/136/13	KOM-ECO S.A., Lublin, ul. Wojenna 3	w związku z kontrolą DIS-K-421/79/13	ustalenia z kontroli wykorzystano w postępowaniu DIS-K-421/79/13
132.	07-11.10.2013 DIS-K-421/137/13	MPO SITA Lublin Sp. z o.o., Lublin, ul. Ciepłownicza 6	w związku z kontrolą DIS-K-421/79/13	ustalenia z kontroli wykorzystano w postępowaniu DIS-K-421/79/13
133.	14-18.10.2013 DIS-K-421/138/13	Software Hauptstadt Sp. z o.o., Sieraków, ul. Towarowa 17	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
134.	07-11. i 15-17.10.2013 DIS-K-421/139/13	Międzyzakładowa Spółdzielnia Mieszkaniowa „Energetyka”, Warszawa, ul. Zwierzyniecka 8a	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
135.	07-11.10.2013 DIS-K-421/140/13	Free4Fresh Sp. z o.o., Warszawa, ul. Jutrzenki 177	w związku z kontrolą DIS-K-421/72/13	decyzja GIODO
136.	08-11.10.2013 DIS-K-421/141/13	Ministerstwo Finansów, Warszawa, ul. Świętokrzyska 12	z urzędu	nie stwierdzono uchybień
137.	14-18.10.2013 DIS-K-421/142/13	Grupa Allegro Sp. z o.o., Wrocław, ul. Śrubowa 1	z urzędu	decyzja GIODO
138.	14-18.10.2013 DIS-K-421/143/13	Skąpiec.pl, Wrocław, ul. Powstańców Śląskich 2-4	z urzędu	w toku
139.	14-18.10.2013 DIS-K-421/144/13	Telewizja Polska S.A., Warszawa, ul. Woronicza 17	z urzędu	nie stwierdzono uchybień
140.	21-25.10.2013 DIS-K-421/145/13	Grupa Onet.pl S.A., Kraków, ul. Zapolskiej 44	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
141.	21-25.10.2013 DIS-K-421/146/13	Miejski Zakład Komunikacji w Toruniu Sp. z o.o., Toruń, ul. Sienkiewicza 24/26	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
142.	21-28.10.2013 DIS-K-421/148/13	Wydział Konsularny Ambasady Rzeczypospolitej Polskiej w Państwie Izrael, Tel Awiw, ul. Soutine 16	z urzędu	w toku
143.	22-28.10.2013 DIS-K-421/149/13	OK System Polska S.A., Warszawa, ul. Tamka 38	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
144.	21.10.2013 DIS-K-421/150/13	Citi Group Sp. z o.o., Warszawa, ul. Foksal 18	Prokuratura Rejonowa w Wysokiem Maz.	decyzja GIODO
145.	28-30.10.2013 DIS-K-421/151/13	TelePolska Sp. z o.o., Warszawa, Al. Jerozolimskie 123a	z urzędu	decyzja GIODO
146.	28-31.10.2013 DIS-K-421/152/13	Chrześcijańska Służba Charytatywna, Warszawa, ul. Foksal 18	Departament Orzecznictwa Legislacji i Skarg	usunięto uchybienia
147.	28-31.10.2013 DIS-K-421/153/13	Lycamobile Sp. z o.o., Warszawa, ul. Rzymowskiego 34 lok. R34	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
148.	28-30.10.2013 DIS-K-421/154/13	Contbus Olszak – Anna Olszak, Stanisław Olszak sp.j.,	Departament Orzecznictwa	w toku

		Lublin, ul. Kolorowa 4/1	Legislacji i Skarg	
149.	04-08.11.2013 DIS-K-421/155/13	Star Typ Sport Zakłady Wzajemne Sp. z o.o., Katowice, ul. Porcelanowa 8	z urzędu	nie stwierdzono uchybień
150.	04-08.11.2013 DIS-K-421/156/13	Komenda Miejska Policji w Poznaniu, Poznań, ul. Szylinga 2	Najwyższa Izba Kontroli	pismo do Komendanta Głównego Policji
151.	12-15.11.2013 DIS-K-421/157/13	Prezydent Miasta Żyrardowa, Żyrardów, Pl. Jana Pawła II nr 1	z urzędu	wystąpienie do Rady Miasta Żyrardowa
152.	12-15.11.2013 DIS-K-421/158/13	Centrum Przetwarzania Danych Ministerstwa Finansów, Radom, ul. Samorządowa 1	z urzędu	nie stwierdzono uchybień
153.	13-15.11.2013 DIS-K-421/159/13	Komenda Rejonowa Policji Warszawa I, Warszawa, ul. Wilcza 21	z urzędu	pismo do Komendanta Głównego Policji
154.	18-20.11.2013 DIS-K-421/160/13	Prima Sp. z o.o., Inowrocław, ul. Magazynowa 92	z urzędu	nie stwierdzono uchybień
155.	18-22.11.2013 DIS-K-421/161/13	Powiatowy Urząd Pracy w Lęborku, Lębork, ul. Gdańska 35	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
156.	18-26.11.2013 DIS-K-421/162/13	Urząd Celny III „Port Lotniczy” w Warszawie, Warszawa, ul. Żwirki i Wigury 1	z urzędu	nie narusza przepisów ustawy o ochronie danych osobowych
157.	18-26.11.2013 DIS-K-421/163/13	Izba Celna w Warszawie, Warszawa, ul. Ciołka 14A	z urzędu	decyzja GIODO
158.	18-22.11.2013 DIS-K-421/164/13	I Liceum Ogólnokształcące im. A. Asnyka, Kalisz, ul. Grodzka 1	Prokuratura Rejonowa w Kaliszu	decyzja GIODO
159.	18-22.11.2013 DIS-K-421/165/13	Urząd Miasta i Gminy Stryków, Stryków, ul. Kościuszki 27	z urzędu	nie stwierdzono uchybień
160.	19-22.11.2013 DIS-K-421/166/13	Nokia Corporation, Warszawa, Rondo ONZ 1	z urzędu	nie ma zastosowania prawo polskie
161.	26-30.11.2013 DIS-K-421/167/13	Wydział Konsularny Ambasady RP w Wilnie, Wilno, ul. Smelio 20A	z urzędu	w toku
162.	25-29.11.2013 DIS-K-421/168/13	Miejskie Przedsiębiorstwo Usług Komunalnych Sp. z o.o., Warszawa, ul. Redutowa 25	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
163.	02-06.12.2013 DIS-K-421/169/13	Wydział Konsularny Ambasady RP w Bratysławie, Bratysława, ul. Hummelova 4	z urzędu	w toku
164.	02-06.12.2013 DIS-K-421/170/13	Hyperion S.A., Warszawa, ul. Żurawia 18	Zespół ds. Naruszeń Danych Osobowych	w toku
165.	02-06.12.2013 DIS-K-421/171/13	Kompania Węglowa S.A. Kopalnia Węgla Kamiennego „Piast”, Bieruń, ul. Granitowa 16	z urzędu	nie stwierdzono uchybień
166.	02-06.12.2013 DIS-K-421/172/13	TKTEX Sp. z o.o., Częstochowa, ul. 1 Maja 21	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
167.	02-06.12.2013 DIS-K-421/173/13	Hyperion Wschód Sp. z o.o., Warszawa, Plac Czerwca 1976 r. nr 4	Zespół ds. Naruszeń Danych Osobowych	w toku
168.	09-13.12.2013 DIS-K-421/174/13	Urząd Marszałkowski Województwa Śląskiego,	z urzędu	decyzja GIODO

		Katowice, ul. Ligonia 46		
169.	09-13.12.2013 DIS-K-421/175/13	MNI Telecom S.A., Radom, ul. Potkanowska 54A	Zespół ds. Naruszeń Danych Osobowych	w toku
170.	09-13.12.2013 DIS-K-421/176/13	Powszechna Agencja Internet „PAI" S.A., Łódź, ul. Kilińskiego 122/128	Zespół ds. Naruszeń Danych Osobowych	w toku
171.	09-12.12.2013 DIS-K-421/177/13	Nowy Ekran S.A., Zalesie k. Piaseczna, ul. Bukowa 12	z urzędu	nie stwierdzono uchybień
172.	16-19.12.2013 DIS-K-421/178/13	Super Pharm Poland Sp. z o.o., Warszawa, ul. Domaniewska 39	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
173.	16-20.12.2013 DIS-K-421/179/13	Medgo Sp. z o.o., Warszawa, Al. Jerozolimskie 65c	z urzędu	decyzja GIODO

Załącznik nr 3

Wykaz orzeczeń wydanych w 2013 r. przez Wojewódzki Sąd Administracyjny w Warszawie i Naczelny Sąd Administracyjny w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych

L.p.	Data/ sygnatura orzeczenia WSA w Warszawie lub NSA	Sygnatura rozstrzygnięcia GIODO	Przedmiot sprawy	Rozstrzygnięcie WSA w Warszawie lub NSA
1.	03.01.2013 r. II SA/Wa 1960/12	DOLiS/DEC-908/12/57995, 58004	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA o zwolnieniu z kosztów sądowych
2.	08.01.2013 r. II SAB/Wa 452/12	GIODO-074-17/10	Skarga na bezczynność w przedmiocie ochrony danych osobowych	Postanowienie WSA o zwolnieniu z kosztów sądowych
3.	08.01.2013 r. II SA/Wa 1655/12	DOLiS/DEC-622/12/42503, 42510	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
4.	9.01.2013 r. II SA/Wa 1475/12	DRZDO/DEC-500/12/34361	Umorzenie postępowania prowadzonego w związku ze zgłoszeniem zmian w zbiorze danych	Oddalenie skargi
5.	9.01.2013 r. II SA/Wa 1476/12	DRZDO/DEC-501/12/34362	Umorzenie postępowania prowadzonego w związku ze zgłoszeniem zmian w zbiorze danych	Oddalenie skargi
6.	09.01.2013 r. II SA/Wa 1010/12	GI-DS-430/614/02	Skarga na niewykonanie przez GIODO wyroku NSA z dnia 29.04.2003 r., sygn. akt II SAB 405/02	Postanowienie WSA – odrzucenie skargi o wymierzenie grzywny - art.154 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi
7.	10.01.2013 I OSK 2029/11	DIS/DEC-18/1483/11	Opcjonalność wyrażenia zgody na przetwarzanie danych osobowych.	Oddalenie skargi
8.	10.01.2013 r. I OSK 2276/11	DOLiS/DEC-84/11/5415,5416	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
9.	10.01.2013 r. I OSK 2383/11	DOLiS/DEC-8/11/439,440,442	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 14.09.2011 r., II SA/Wa 645/11, w sprawie ze skargi na decyzję w przedmiocie odmowy uwzględnienia wniosku o zabezpieczenie danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
10.	15.01.2013 r. II SA/Wa 1433/12	DOLiS/DEC-508/12/35328, 35333	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi

11.	17.01.2013 r. II SA/Wa 1425/12	DOLiS/DEC-452/12/31599, 31605,31611, 31618	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku o nakazanie usunięcia danych osobowych ze zbioru danych	Postanowienie WSA o zwolnieniu z kosztów sądowych
12.	17.01.2013 r. II SA/Wa 1873/12	DOLiS/POST-281/12/48585, 48588,48590	skarga na postanowienie w przedmiocie niedopuszczalności wniosku o ponowne rozpatrzenie sprawy	Wyrok WSA – oddalenie skargi
13.	18.01.2013 r. II SA/Wa 2106/12	DOLiS/DEC-832/12/53856, 53861,53863,	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o zwolnieniu z kosztów sądowych
14.	24.01.2013 I OSK 1827/11	DIS/DEC-43/2827/11	Dopełnienie obowiązku informacyjnego wynikającego z art. 25 ust. 1 ustawy.	Uchylenie zaskarżonego wyroku WSA w Warszawie z dnia 2.06.2011 sygn. II SA/Wa 720/11 i przekazanie sprawy do ponownego rozpoznania
15.	24.01.2013 r. II SA/Wa 1242/12	DOLiS/DEC-373/12/27562, 27570	Skarga na decyzję w przedmiocie nakazu udostępnienia danych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
16.	25.01.2013 r. II SA/Wa 1889/12	DOLiS/DEC-750/12/49111, 49115,49118	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
17.	29.01.2013 r. II SA/Wa 1445/12	DOLiS/POST-145/12/31133, 31134	Skarga na postanowienie w przedmiocie odmowy wyjaśnienia wątpliwości co do treści decyzji	Wyrok WSA – oddalenie skargi
18.	31.01.2013 r. II SA/Wa 1112/12	DOLiS/DEC-318/12/23575, 23580,23585	Skarga na decyzję w przedmiocie nakazu udostępnienia danych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
19.	31.01.2013 r. II SA/Wa 2734/11	DOLiS/DEC-720/11/40257, 40262	Skarga na decyzję w przedmiocie nakazu udostępnienia danych	Wyrok WSA – oddalenie skargi
20.	04.02.2013 r. II SAB/WA 422/11	DOLiS-440-21/12	Skarga w przedmiocie przewlekłości postępowania w sprawie przetwarzania danych	Wyrok WSA - przewlekłość postępowania nie miała miejsca z rażącym naruszeniem prawa, w pozostałym zakresie - umorzenie postępowania
21.	04.02.2013 r. II SA/Wa 1530/12	DOLiS/DEC-531/12/36278, 36280	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
22.	05.02.2013 r. II SA/Wa 1842/12	DOLiS/DEC-725/12/47555, 47558	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
23.	07.02.2013 r. II SA/Wa 29/13	DOLiS/POST-394/12/77551, 77555	Skarga na postanowienie w przedmiocie niedopuszczalności wniosku o ponowne rozpatrzenie sprawy	Postanowienie WSA – odrzucenie skargi
24.	07.02.2013 r. II SA/Wa 1986/12	DOLiS/DEC-903/12/57941, 57948	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
25.	11.02.2013 r. II SA/Wa 2063/12	DOLiS/DEC-865/12/55801,	Skarga na decyzję w przedmiocie przetwarzania	Postanowienie WSA - odmawiające zwolnieniaz kosztów sądowych

		55802,55803, 55804	danych osobowych	
26.	12.02.2013 r. II SA/Wa 2556/12	DOLiS/DEC-743/11/41150, 41152,41154, 41155,41168	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o podjęciu zawieszonego postępowania
27.	13.02.2013 r. II SA/Wa 1654/12	DOLiS/DEC-652/12/43574, 43575	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
28.	13.02.2013 r. II SA/Wa 1843/12	DOLiS/DEC-822/12/53801, 53802	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
29.	13.02.2013 r. II SA/Wa 1921/12	DOLiS/DEC-784/12/51085, 51091	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
30.	14.02.2013 r. II SA/Wa 2173/12	DOLiS/DEC-911/12/58456, 58468	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
31.	19.02.2013 r. I OSK 906/12	DOLiS/DEC-452/11/26463, 26466	Skarga kasacyjna od wyroku WSA z 28.11.2012 r. II SA/Wa 1875/11, oddalającego skargę na decyzję w przedmiocie ochrony danych	Postanowienie NSA o umorzeniu postępowania
32.	20.02.2013 r. II SA/Wa 152/13	DOLiS/DEC-1097/12/69181, 69183	Skarga na decyzję w przedmiocie nakazu udostępnienia danych	Postanowienie WSA – wstrzymanie wykonania decyzji
33.	20.02.2013 r. I OSK 3268/12	DOLiS/DEC-1383/10/50305, 50306,50309	Skarga kasacyjna od wyroku WSA z dnia 7.10.2011 r. II SA/Wa 364/11 oddalającego skargę na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjna
34.	25.02.2013 r. II SA/Wa 2267/12	DOLiS/DEC-996/12/62407, 62423,62429, 62431	Skarga na decyzję w przedmiocie nakazania udostępnienia danych	Postanowienie WSA – oddalenie skargi
35.	27.02.2013 r. II SA/Wa 1557/12	DOLiS/POST-159/12/36660, 36662,36665, 36669	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku o wydanie uwierzytelnionych odpisów dokumentów z akt sprawy	Postanowienie WSA – oddalenie skargi
36.	27.02.2013 r. II SA/Wa 1206/12	DOLiS/DEC-379/12/27595, 27600	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA - odmawiające zwolnienia z kosztów sądowych
37.	27.02.2013 r. II SA/Wa 2296/12	DOLiS/POST-315/12/53547	Skarga na postanowienie o odmowie wszczęcia postępowania	Postanowienie WSA - odmowa zwolnieniaz kosztów sądowych
38.	28.02.2013 r. II SA/Wa 911/12	DOLiS/DEC-267/12/20419, 20427,20431	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o zwolnieniu z kosztów sądowych
39.	04.03.2013 r. II SA/Wa 2218/12	DOLiS/DEC-990/12/62382, 62385	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Wyrok WSA – oddalenie skargi
40.	05.03.2013 r.	DOLiS/DEC-	Skarga na decyzję	Wyrok WSA – oddalenie skargi

	II SA/Wa 1796/12	727/12/47540, 47542	w przedmiocie nakazania spełnienia obowiązku informacyjnego poprzez podanie treści danych osobowych	
41.	05.03.2013 r. II SA/Wa 267/11	DOLiS/DEC-1310/10/47273, 47275,47277	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 7.06.2011 r. II SA/Wa 267/11 oddalającego skargę na decyzję w przedmiocie nakazu usunięcia uchybień powstałych w procesie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi kasacyjnej
42.	06.03.2013 r. II SA/Wa 32/13	DOLiS/DEC-1060/12/66556, 66559	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
43.	06.03.2013 r. II SA/Wa 1783/12	DOLiS/DEC-693/12/46820, 46827,46830	Skarga na decyzję w przedmiocie odmowy stwierdzenia nieważności decyzji GIODO	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
44.	07.03.2013 r. II SA/Wa 2265/12	DOLiS/DEC-1066/12/66593, 66597	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
45.	08.03.2013 r. II SA/Wa 137/13	DOLiS-440-974/10	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – uchylenie postanowienia WSA w Warszawie z dnia 19.10.2012 r. w przedmiocie stwierdzenia prawomocności postanowienia WSA w Warszawie z dnia 23.04.2012 r. o sygn. II SA/Wa 455/12
46.	12.03.2013 r. II SA/Wa 2126/12	DOLiS/POST-327/12/57034	Skarga na postanowienie w przedmiocie odmowy sporządzenia odpisów wszystkich dokumentów znajdujących się w aktach sprawy dotyczącej ochrony danych osobowych	Wyrok WSA – oddalenie skargi
47.	13.03.2013 r. I OSK 2344/12	DOLiS/POST-252/11/56551	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 27.06.2012 r. II SA/Wa 121/12 oddalający skargę na postanowienie w przedmiocie oddalenia skargi na bezczynność polegającą na niepodjęciu czynności zmierzających do zastosowania środków egzekucyjnych	Wyrok NSA – oddalenie skargi kasacyjnej
48.	14.03.2013 I OSK 1059/12	DIS/DEC-595/34725/11	Przetwarzanie danych osobowych przez wspólnotę mieszkaniową.	Oddalenie skargi
49.	14.03.2013 r. II SA/Wa 149/13	DOLiS/DEC-1180/12/72653, 72655	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA o zwolnieniu z kosztów sądowych
50.	14.03.2013 r.	DOLiS/DEC-	Skarga kasacyjna od wyroku	Wyrok NSA – oddalenie skargi

	I OSK 620/12	459/11/26524, 26548	WSA w Warszawie z dnia 24.11.2011 r. II SA/Wa 1828/11 oddalającego skargę na decyzję w przedmiocie nakazania wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych	kasacyjnej
51.	14.03.2013 r. II SA/Wa 2734/11	DOLiS/DEC-720/11/40257, 40262	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA o sprostowaniu omyłki pisarskiej w komparycji wyroku WSA w Warszawie z dnia 31.01.2013 r. II SA/Wa 2734/11
52.	15.03.2013 r. II SA/Wa 2106/12	DOLiS/DEC-832/12/53856, 53861,53863	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
53.	15.03.2013 r. II SAB/Wa 452/12	GIODO-074-17/10	Skarga na bezczynność w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
54.	18.03.2013 r. II SA/Wa 2232/12	DOLiS/DEC-965/12/61053, 61055	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
55.	20.03.2013 r. II SA/Wa 137/13	DOLiS/DEC-14/12/882,884	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
56.	20.03.2013 r. II SA/Wa 251/13	DOLiS/DEC-1181/12/72849, 72851	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku i umorzenia postępowania	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
57.	22.03.2013 r. II SA/Wa 2328/12	DOLiS/DEC-625/13/37430, 37431	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA zawieszające postępowanie
58.	22.03.2013 r. II SA 307/13	DOLiS/DEC-743/11/41150, 41152,41154, 41155,43168	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA oddalające wniosek o wyłączenie sędziego
59.	22.03.2013 r. I OSK 597/12	DOLiS/DEC-336/11/19849, 19854	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 7.12.2011 r. II SA/Wa 1560/11 w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
60.	22.03.2013 r. I OSK 813/12	DOLiS/DEC-515/08/22854, 22857	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 19.12.2011 r. II SA/Wa 2209/11 oddalający skargę na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
61.	22.03.2013 r. II SAB/Wa 515/12	DOLiS-067-41/12	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku o udostępnienie informacji publicznej	Wyrok WSA – oddalenie skargi
62.	22.03.2013 r. II SAB/Wa 514/12	DOLiS-067-42/12	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku o udostępnienie informacji publicznej	Wyrok WSA – oddalenie skargi

63.	25.03.2013 r. II SAB/Wa 96/13	DOLiS-440-742/12	Skarga na bezczynność w przedmiocie rozpatrzenia wniosku o udostępnienie danych osobowych	Postanowienie WSA – odrzucenie skargi
64.	27.03.2013 r. I OSK 1047/12	DOLiS/DEC-334/11/19326, 19327,19329	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 2.12.2011 r. II SA/Wa 1484/11 oddalający skargę na decyzję w przedmiocie odmowy uwzględnienia wniosku	Wyrok NSA – oddalenie skargi kasacyjnej
65.	27.03.2013 r. I OSK 633/12	DOLiS/DEC-328/11/18882, 18883	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 15.11.2011 r. II SA/Wa 1500/11 oddalającego skargę na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
66.	27.03.2013 r. I OSK 1060/12	DOLiS/DEC-786/11/43365, 43366	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 21.02.2012 r. II SA/Wa 2350/11 oddalającego skargę na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA – uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania przez WSA w Warszawie
67.	27.03.2013 r. I OSK 932/12	DOLiS/DEC-377/11/23002, 23008	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 20.01.2012 r. II SA/Wa 1671/11 oddalającego skargę na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania przez WSA w Warszawie
68.	04.04.2013 r. II SA/Wa 189/13	DOLiS/DEC-1170/12/71238, 71242	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na odmowę udostępnienia danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
69.	04.04.2013 r. I OSK 897/12	DOLiS/DEC-668/11/37533, 37540	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 11.01.2012 r. II SA/Wa 2026/11 oddalającego skargę na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania przez WSA w Warszawie
70.	08.04.2013 r. II SA/Wa 254/13	DOLiS/DEC-1213/12/74334, 74336	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
71.	08.04.2013 r. II SAB/Wa 117/13	DOLiS-440-1122/12	Skarga na naruszenie przepisów dotyczących ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
72.	09.04.2013 II SA/Wa 211/13	DIS/DEC-112/12/7893	Niezgłoszenie do rejestracji zbioru danych zebranych poprzez system monitoringu wizyjnego	Oddalenie skargi
73.	09.04.2013 r. II SA/Wa 605/13	DOLiS/DEC-53/13/3763,3766, 3773	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
74.	10.04.2013 r. II SA/Wa 1083/12	DOLiS/DEC-295/12	Skarga na decyzję w przedmiocie przetwarzania	Postanowienie WSA o przyznaniu pomocy w zakresie ustanowienia

			danych osobowych	pełnomocnika
75.	10.04.2013 r. II SA/Wa 1960/12	DOLiS/DEC-908/12/57995, 58004	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Wyrok WSA – oddalenie skargi
76.	10.04.2013 r. I OSK 2770/12	DOLiS/DEC-508/12/35328, 35333	skarga GIODO o wznowienie postępowania zakończonego wyrokiem NSA z dnia 17.07.2012 r. I OSK 130/12 oddalającym skargę kasacyjną GIODO od wyroku WSA w Warszawie z dnia 12.10.2011 r. II SAB/Wa 170/11 w sprawie ze skargi na bezczynność organu w przedmiocie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi o wznowienie postępowania
77.	12.04.2013 r. II SA/Wa 1425/12	DOLiS/DEC-452/12/31599, 31605,31611, 31618,31623	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
78.	12.04.2013 r. II SA/Wa 2261/12	DOLiS/DEC-992/12/62381, 62386	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
79.	16.04.2013 r. II SA/Wa 293/13	DOLiS/DEC-1255/12/77408, 77409	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA - odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
80.	17.04.2013 r. II SA/Wa 284/13	DOLiS/DEC-1204/12/74357, 74360	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
81.	17.04.013 r. II SA/Wa 1144/12	DOLiS/DEC-374/12/27588, 27592	Skarga na decyzję przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
82.	17.04.2013 r. II SA/Wa 191/13	DOLiS/DEC-731/08	Skarga o wymierzenie GIODO grzywny z tytułu niewykonania wyroku WSA w Warszawie z dnia 15.11.2010 r. II SA/Wa 1477/10	Wyrok WSA – oddalenie skargi o wymierzenie grzywny - art. 154 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi
83.	17.04.2013 r. II SA/Wa 125/13	DOLiS-440-292/12	Skarga na przewlekłe prowadzenie postępowania w przedmiocie niewypełnienia obowiązku informacyjnego	Postanowienie WSA – odrzucenie skargi
84.	18.04.2013 r. II SA/Wa 190/13	DOLiS/DEC-1166/12/71143, 71149,71151, 71159	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
85.	19.04.2013 r. II SA/Wa 419/13	DOLiS/DEC-1258/12/77490, 77492	Skarga na decyzję w przedmiocie usunięcia danych	Postanowienie WSA – odmowa wstrzymania wykonania decyzji
86.	19.04.2013 r. II SA/Wa 2107/12	DOLiS/DEC-883/12/56856, 56858	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
87.	19.04.2013 r.	DOLiS/DEC-	Skarga na decyzję	Wyrok WSA – oddalenie skargi

	II SA/Wa 2266/12	1052/12/65087, 65089	w przedmiocie ochrony danych osobowych	
88.	19.04.2013 r. II SAB/Wa 452/12	GIODO-074-17/10	Skarga na bezczynność w przedmiocie ochrony danych osobowych	Postanowienie WSA - przyznanie na rzecz adwokata określonej kwoty ze środków budżetowych WSA w Warszawie, tytułem nieopłaconej pomocy prawnej świadczonej z urzędu
89.	19.04.2013 r. II SA/Wa 2734/11	DOLiS/DEC-720/11/40257, 40262	Skarga na decyzję w przedmiocie udostępnienia danych	Postanowienie WSA - przyznanie na rzecz adwokata określonej kwoty ze środków budżetowych WSA w Warszawie, tytułem nieopłaconej pomocy prawnej świadczonej z urzędu
90.	22.04.2013 r. II SA/Wa 1582/11	DOLiS/DEC-450/11/26448, 26449	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
91.	23.04.2013 r. II SA/Wa 320/13	DOLiS/DEC-1198/12/74269, 74273	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
92.	23.04.2013 r. I OZ 269/13	DOLiS/DEC-1097/12/69181, 69183	Skarga na decyzję w przedmiocie udostępnienia danych	Postanowienie NSA – oddalenie zażalenia GIODO na postanowienie WSA w Warszawie z dnia 20.02.2013 r. o wstrzymaniu wykonania zaskarżonej decyzji
93.	24.04.2013 II SA/Wa 507/13	DIS/DEC-43/2827/11	Dopełnienie obowiązku informacyjnego wynikającego z art. 25 ust. 1 ustawy o ochronie danych osobowych	Uchylenie zaskarżonej decyzji, decyzja nie podlega wykonaniu w całości
94.	24.04.2013 r. II SA/Wa 160/11	DOLiS/DEC-1318/10/47328, 47329	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
95.	26.04.2013 r. II SA/Wa 710/09	DOLiS/DEC-176/09	Skarga na decyzję w przedmiocie odmowy wznowienia postępowania	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
96.	26.04.2013 r. II SA/Wa 575/10	DOLiS/DEC-254/07	Skarga na decyzję w przedmiocie odmowy nakazania sprostowania danych o stanie zdrowia	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
97.	08.05.2013 r. II SA/Wa 756/13	DOLiS/DEC-133/13/8353,8356	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
98.	09.05.2013 r. II SAB/Wa 134/13	DOLiS-440-954/12	Skarga na przewlekłe prowadzenie postępowania w przedmiocie skargi dotyczącej udostępnienia danych osobowych	Postanowienie WSA – odrzucenie skargi
99.	14.05.2013 r. II SA/Wa 742/13	DOLiS/DEC-182/13/10117,	Skarga na decyzję w przedmiocie ochrony danych	Postanowienie WSA – przyznanie prawa pomocy w zakresie

		10120	osobowych	zwolnienia od kosztów sądowych
100.	15.05.2013 r. II SA/Wa 2063/12	DOLiS/DEC-865/12/55801, 55802,55803, 55804	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
101.	16.05.2013 r. II SA/Wa 911/12	DOLiS/DEC-267/12/20419, 20427,20431	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
102.	17.05.2013 r. II SA/Wa 735/13	DOLiS/DEC-117/13/8319,8320	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania decyzji
103.	17.05.2013 r. II SA/Wa 2328/12	DOLiS/DEC-1037/12/64659, 64661	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o podjęciu zawieszonego postępowania
104.	22.05.2013 r. II SA/Wa 450/13	DOLiS/DEC-55/13/3819,3823, 3824,3828,3840	Skarga na decyzję organu	Postanowienie WSA – odrzucenie zażalenia na zarządzenie Przewodniczącego Wydziału II WSA w Warszawie o przesłaniu do wypełnienia formularza wniosku o przyznanie prawa pomocy
105.	22.05.2013 r. II SA/Wa 416/13	DOLiS/DEC-50/13/3732,3734, 3736	Skarga na decyzję w przedmiocie odmowy uwzględnienia skargi o przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
106.	22.05.2013 r. II SA/Wa 1960/12	DOLiS/DEC-908/12/57995, 58004	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA – sprostowanie omyłki pisarskiej
107.	22.05.2013 r. II SA/Wa 2106/12	DOLiS/DEC-832/12/53856, 53861,53863	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Postanowienie WSA – przywrócenie terminu do zgłaszania wniosku o uzasadnienie wyroku
108.	23.05.2013 r. II SA/Wa 625/13	DOLiS/DEC-56/13/3855,3857, 3859	Skarga na decyzję w przedmiocie odmowy uwzględnienia skargi o przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
109.	24.05.2013 r. II SA/Wa 523/13	DOLiS/POST-9/13/429	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania w sprawie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
110.	27.05.2013 r. II SA/Wa 293/13	DOLiS/DEC-1255/12/77408, 77409	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie sprzeciwu od postanowienia referendarza sądowego z dnia 16.04.2013 r. o odmowie przyznania prawa pomocy
111.	27.05.2013 r. II SA/Wa 487/13	DOLiS/DEC-49/13/3720,3721, 3722,3723,3724	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
112.	28.05.2013 r. I OSK 315/13	DOLiS-440-275/12 DOLiS-956/09	Skarga kasacyjna od wyroku WSA w Warszawie dnia 21.08.2012 r. II SA/Wa 831/12	Wyrok NSA – oddalenie skargi kasacyjnej

			w sprawie niewykonania przez organ wyroku WSA w Warszawie z dnia 14.10.2010 r. II SAB/Wa 137/10	
113.	29.05.2013 r. II SA/Wa 1019/10	DOLiS/DEC-571/10	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 26.10.2010 r. II SA/Wa 1019/10 oddalającego skargę na decyzję w przedmiocie stwierdzenia nieważności decyzji	Postanowienie WSA – odrzucenie skargi kasacyjnej
114.	31.05.2013 r. II SA/Wa 2209/11	DOLiS/DEC-835/10	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA o przyznaniu adwokatowi ze środków udżetowych WSA w Warszawie, wynagrodzenia za zastępstwo prawne wykonane na zasadzie prawa pomocy
115.	06.06.2013 r. II SA/Wa 29/13	DOLiS/POST-361/12/65266, 65267	Skarga na postanowienie w przedmiocie uchybienia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy	Postanowienie WSA – sprostowanie omyłki pisarskiej
116.	7.06.2013 r. II SA/Wa 666/13	DRZDO/DEC-76/13/5614	Odmowa rejestracji zbioru danych osobowych	Oddalenie skargi
117.	07.06.2013 r. II SA/Wa 123/13	DOLiS/POST-315/12/53547	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
118.	07.06.2013 r. II SA/Wa 123/13	DOLiS/POST-315/12/53547	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – oddalenie wniosku o przyznanie prawa pomocy w zakresie całkowitym obejmującym zwolnienie od kosztów sądowych i ustanowienie radcy prawnego
119.	10.06.2013 r. II SAB/Wa 145/13	DOLiS-440-1162/12	Skarga na przewlekłe prowadzenie przez GIODO postępowania w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż przewlekłość postępowania miała miejsce z rażącym naruszeniem prawa i wymierzający organowi grzywnę w wysokości 1000 złotych, zaś w pozostałym zakresie umorzono postępowanie
120.	10.06.2013 r. II SA/Wa 797/13	DOLiS/DEC-377/11/23002, 23008	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – umorzenie postępowania z art. 161 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi
121.	11.06.2013 r. II SA/Wa 1590/12	DOLiS/DEC-577/12/39478, 39479,39480	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – przyznanie prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
122.	17.06.2013 r. II SA/Wa 2296/12	DOLiS/POST-365/12/65640	Skarga	Postanowienie WSA – odrzucenie skargi
123.	17.06.2013 r. II SA/Wa 2296/12	DOLiS/POST-365/12/65640	Skarga	Postanowienie WSA – oddalenie wniosku o przyznanie prawa pomocy w zakresie całkowitym obejmującym zwolnienie od kosztów sądowych oraz ustanowienie radcy prawnego

124.	17.06.2013 r. II SA/Wa 152/13	DOLiS/DEC-1097/12/69181, 69183	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
125.	18.06.2013 r. II SA/Wa 812/13	DOLiS/DEC-1311/10/47279, 47283	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całości
126.	20.06.2013 r. II SA/Wa 969/11	DOLiS/DEC-143/11/8238,8239	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – przyznanie radcy prawnemu ze środków budżetowych WSA w Warszawie wynagrodzenia za zastępstwo prawne wykonane na zasadzie prawa pomocy
127.	21.06.2013 r. II SA/Wa 307/13	DOLiS/DEC-743/11/41150,41152,41154,41155, 41168	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
128.	25.06.2013 r. II SA/Wa 1083/12	DOLiS/DEC-295/12	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 14.12.2012 r., II SA/Wa 1083/12, oddalającego skargę na decyzję w przedmiocie odmowy uchylenia decyzji w sprawie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi kasacyjnej
129.	26.06.2013 r. II SA/Wa 710/09	DOLiS/DEC-176/09	Skarga na decyzję w przedmiocie odmowy wznowienia postępowania administracyjnego	Postanowienie WSA – odrzucenie sprzeciwu od postanowienia referendarza sądowego z dnia 26.04.2013 r. o odmowie przyznania prawa pomocy
130.	26.06.2013 r. II SA/Wa 978/13	DOLiS/DEC-293/13/16103, 16106	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
131.	26.06.2013 r. I OZ 527/13	DOLiS/DEC-1255/12/77408, 77409	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 27.05.2013 r., II SA/Wa 293/13, o odrzuceniu sprzeciwu od postanowienia referendarza sądowego z dnia 16.04.2013 r. o odmowie przyznania prawa pomocy
132.	26.06.2013 r. II SA/Wa 575/10	DEC-DOLiS-254/07	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku o nakazie sprostowania danych o stanie zdrowia	Postanowienie WSA – odrzucenie sprzeciwu od postanowienia referendarza sądowego z dnia 26.04.2013 r. o odmowie przyznania prawa pomocy
133.	27.06.2013 r. II SA/Wa 101/13	DOLiS/DEC-1161/12/70957, 70958	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – oddalenie wniosku o wyłączenie sędziego
134.	27.06.2013 r. II SA/Wa 1582/11	DOLiS/DEC-450/11/26448, 26449	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na odmowę udostępnienia danych	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
135.	27.06.2013 r. II SA/Wa 1582/11	DOLiS/DEC-450/11/26448,	Skarga na decyzję w przedmiocie odmowy	Postanowienie WSA – przywrócenie terminu do wniesienia zażalenia od

		26449	uwzględnienia wniosku na odmowę udostępnienia danych	postanowienia WSA w Warszawie z dnia 3.04.2012 r., II SA/Wa 1582/11, o odmowie sporządzenia uzasadnienia wyroku
136.	27.06.2013 r. II SAB/Wa 223/13	DOLiS-035-617/13	Skarga na bezczynność GIODO w przedmiocie rozpatrzenia pisma dotyczącego ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
137.	04.07.2013 r. II SO/Wa 55/13	DOLiS/DEC-1318/10	Skarga na decyzję	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
138.	09.07.2013 r. II SA/Wa 449/13	DOLiS/DEC-83/12/6241,6243	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
139.	11.07.2013 r. II SA/Wa 1194/13	DOLiS/POST-127/13/29233, 29244	Skarga na postanowienie w przedmiocie stwierdzenia uchybienia terminu do złożenia wniosku o ponowne rozpatrzenie sprawy	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
140.	15.07.2013 r. II SA/Wa 2209/11	DOLiS/DEC-515/08/22854, 22857	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – sprostowanie błędu rachunkowego w punkcie 2 sentencji wyroku WSA w Warszawie z dnia 19.12.2011 r., II SA/Wa 2209/11
141.	17.07.2013 r. II SA/Wa 815/13	DOLiS/DEC-263/13/13825, 13832	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku dotyczącego nieprawidłowości w procesie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
142.	17.07.2013 r. II SA/Wa 710/09	DOLiS/DEC-176/09	Skarga na decyzję w przedmiocie odmowy wznowienia postępowania administracyjnego	Postanowienie WSA – uchylenie postanowienia WSA w Warszawie z dnia 26.06.2013 r., II SA/Wa 710/09
143.	18.07.2013 r. II SA/Wa 978/13	DOLiS/DEC-293/13/16103, 16106	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – zwrócenie kwoty wpisanej do rejestru opłat sadowych WSA w Warszawie tytułem zwrotu uiszczonego wpisu
144.	23.07.2013 r. II SA/Wa 597/13	DOLiS/DEC-4/13/138,140	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych
145.	24.07.2013 r. II SA/Wa 806/13	DOLiS/POST-57/13/11637, 11639	Skarga na postanowienie w przedmiocie niedopuszczalności wniosku	Wyrok WSA – uchylenie zaskarżonego postanowienia i określenie, że nie podlega wykonaniu w całości
146.	24.07.2013 r. II SA/Wa 1082/13	DOLiS/DEC-376/13/20434, 20436	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
147.	24.07.2013 r. II SA/Wa 419/13	DOLiS/DEC-1258/12/77490, 77492	Skarga na decyzję w przedmiocie usunięcia danych	Wyrok WSA – oddalenie skargi
148.	25.07.2013 r. II SA/Wa 1047/13	DOLiS/DEC-668/11/37533,	Skarga na decyzję w przedmiocie ochrony danych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz utrzymanej

		37540	osobowych	nią w mocy decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
149.	30.07.2013 r. II SA/Wa 979/13	DOLiS/DEC-367/13/20031, 20036	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
150.	06.08.2013 r. II SO/Wa 53/13	DOLiS/DEC-1318/10	Skarga na decyzję	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
151.	07.08.2013 r. II SA/Wa 2328/12	DOLiS/DEC-1037/12/64659, 64661	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
152.	13.08.2013 r. II SA/Wa 293/13	DOLiS/DEC-1255/12/77408, 77409	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - ustanowienie adwokata w ramach przyznania prawa pomocy, a także odmowa zwolnienia od kosztów sądowych
153.	13.08.2013 r. II SA/Wa 149/13	DOLIS/DEC-1180/12/72653, 72655	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
154.	13.08.2013 r. II SA/Wa 974/13	DOLiS/DEC-957/12/60647, 60651,60652	Skarga na decyzję w przedmiocie umorzenia postępowania	Postanowienie WSA - przyznanie prawa pomocy w zakresie ustanowienia pełnomocnika i odmowa w zakresie zwolnienia od kosztów sądowych
155.	21.08.2013 I OSK 1760/13	DIS/DEC-847/12/55105	Usunięcie danych osobowych.	Odmowa wstrzymania wykonania decyzji
156.	21.08.2013 r. I OSK 1666/12	DOLiS/DEC-885/11/50687, 50693	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 8.03.2012 r., II SA/Wa 2821/11 w sprawie ze skargi na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
157.	21.08.2013 r. I OSK 1661/13	DOLiS/DEC-1198/12/74269, 74273	Skarga kasacyjna od postanowienia WSA w Warszawie z dnia 23.04.2013 r., II SA/Wa 320/13 odrzucającego skargę w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
158.	28.08.2013 r. II SA/Wa 1229/13	DOLiS/DEC-786/11/43365, 43366	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
159.	29.08.2013 r. II SA/Wa 756/13	DOLiS/DEC-133/13/8353,8356	Skarga na decyzję w przedmiocie udostępnienia danych	Wyrok WSA – uchylenie zaskarżonej decyzji, stwierdzenie nieważności poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości
160.	30.08.2013 r.	DOLiS/DEC-	Skarga na decyzję	Postanowienie WSA – przyznanie

	II SA/Wa 293/13	1255/1277408, 77409	w przedmiocie przetwarzania danych osobowych	prawa pomocy w zakresie ustanowienia pełnomocnika, odmowa w zakresie zwolnienia od kosztów sądowych
161.	30.08.2013 r. II SAB/Wa 321/13	DOLiS-067-43/12	Skarga na bezczynność GIODO w przedmiocie rozpoznania wniosku o udostępnienie informacji publicznej	Postanowienie WSA – odrzucenie skargi
162.	05.09.2013 r. II SA/Wa 735/13	DOLiS/DEC-117/13/8319,8320	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok WSA – oddalenie skargi
163.	05.09.2013 r. II SA/Wa 764/13	DOLiS/DEC-181/13/10107, 10110	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
164.	05.09.2013 r. II SAB/Wa 59/12	DOLiS-440-876/11	Skarga w sprawie o wznowienie postępowania zakończonego prawomocnym postanowieniem WSA w Warszawie z dnia 13.03.2012 r., II SAB/Wa 59/12	Postanowienie WSA – przyznanie adwokatowi ze środków budżetowych WSA w Warszawie wynagrodzenia za zastępstwo prawne wykonane na zasadzie prawa pomocy
165.	10.09.2013 r. II SA/Wa 1400/13	DOLiS/DEC-592/13/33390, 33395	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji oraz poprzedzającą jej decyzji
166.	12.09.2013 r. II SA/Wa 710/09	DOLiS/DEC-176/09	Skarga na decyzję w przedmiocie odmowy wznowienia postępowania	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika
167.	13.09.2013 r. I OZ 760/13	DOLiS/DEC-55/13/3819,3823, 3824,3828,3840	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie NSA – oddalono zażalenie na zarządzenie Przewodniczącego Wydziału II WSA w Warszawie z dnia 15.07.2013 r., II SA/Wa 450/13, o wezwaniu do uiszczenia wpisu od skargi
168.	17.09.2013 r. II SA/Wa 1568/13	DOLiS/DEC-609/13/ 35406/35422/ 35430/35434/ 35443/35448/ 35451/35455/ 35458/35461/ 35465/35470	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
169.	17.09.2013 r. II SA/Wa 1664/13	DOLiS/DEC-589/13/33413, 33421	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
170.	17.09.2013 r. II SA/Wa 976/13	DOLiS/DEC-314/13/17450, 17451,17452, 17457	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – oddalenie wniosku o zwolnienie od kosztów sądowych
171.	17.09.2013 r.	DOLiS-440-	Skarga na bezczynność	Postanowienie WSA – odrzucenie

	II SAB/Wa 410/13	185/10	GIODO w przedmiocie rozpatrzenia wniosku o stwierdzenie nieważności decyzji	skargi
172.	17.09.2013 r. II SA/Wa 1521/13	DOLiS/DEC-693/12/46820, 46827,46830	Skarga na decyzję	Postanowienie WSA – odrzucenie skargi o wymierzenie grzywny (art.154 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi
173.	18.09.2013 r. II SA/Wa 742/13	DOLiS/DEC-182/13/10117, 10120	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
174.	18.09.2013 r. I OZ 776/13	DOLiS/DEC-295/12	Skarga na decyzję w przedmiocie odmowy uchylenia decyzji w sprawie przetwarzania danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 25.06.2013 r., II SA/Wa 1083/12, odrzucające skargę kasacyjną od wyroku WSA w Warszawie z dnia 14.12.2012 r., II SA/Wa 1083/12
175.	20.09.2013 r. II SA/Wa 814/13	DOLiS/DEC-82/13/5890,5901	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na nieprawidłowości w procesie przetwarzania danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych
176.	24.09.2013 r. II SA/Wa 1546/13	DOLiS/DEC-593/13/	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
177.	26.09.2013 r. I OZ 796/13	DOLiS/DEC-450/11/26448, 26449	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 3.04.2012 r., II SA/Wa 1582/11 o odmowie sporządzenia uzasadnienia wyroku tego Sądu z dnia 14.12.2011 r., II SA/Wa 1582/1
178.	26.09.2013 r. I OZ 661/13	DOLiS/DEC-450/11/26448, 26449	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie NSA – uchylenie postanowienia WSA w Warszawie z dnia 27.06.2013 r., II SA/Wa 1582/11 o odmowie przyznania prawa pomocy w zakresie całkowitym i przekazanie sprawy do ponownego rozpoznania przez ten Sąd
179.	02.10.2013 r. II SA/Wa 627/13	DOLiS/DEC-110/13/7457,7461	Skarga na decyzję w przedmiocie nakazu wyeliminowania nieprawidłowości w procesie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
180.	02.10.2013 r. II SA/Wa 1057/13	DOLiS/DEC-593/13/33412,33418,33423,33425, 33429	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – umorzenie postępowania z art. 161 ustawy PoPPSA
181.	08.10.2013 r. II SA/Wa 254/13	DOLiS/DEC-1213/12/74334, 74336	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie,

				że zaskarżona decyzja nie podlega wykonaniu w całości
182.	08.10.2013 r. II SA/Wa 977/13	DOLiS/DEC-364/13/19780, 19781	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
183.	09.10.2013 r. II SA/Wa 101/13	DOLiS/DEC-1161/12/70953, 70957	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
184.	09.10.2013 r. II SA/Wa 1401/13	DOLiS/DEC-657/13/38688, 38692	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
185.	10.10.2013 r. II SA/Wa 648/13	DOLiS/DEC-62/13/4071,4074, 4076	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
186.	10.10.2013 r. II SA/Wa 950/13	DOLiS/POST-75/13/16379, 16398	Skarga na postanowienie w przedmiocie niedopuszczalności wniosku o ponowne rozpatrzenie sprawy	Wyrok WSA- - uchylenie zaskarżonego postanowienia i stwierdzenie, że nie podlega wykonaniu w całości
187.	15.10.2013 r. II SA/Wa 1083/12	DOLiS/DEC-295/12	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie wniosku o przywrócenie terminu do wniesienia skargi kasacyjnej
188.	16.10.2013 r. II SAB/Wa 179/13	DOLiS-440-380/12	Skarga na przewlekłe prowadzenie postępowania w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż przewlekłość postępowania miała miejsce z rażącym naruszeniem prawa i wymierzający organowi grzywnę w wysokości 1500 złotych
189.	17.10.2013 r. II SA/Wa 1019/10	DOLiS/DEC-571/10	Skargę na decyzję w przedmiocie stwierdzenia nieważności decyzji	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
190.	18.10.2013 r. I OSK 1195/13	DOLiS/POST-145/12/34133, 34134	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 29.01.2013 r., II SA/Wa 1445/12 w sprawie ze skargi na postanowienie w przedmiocie odmowy wyjaśnienia wątpliwości co do treści decyzji	Wyrok NSA – oddalono skargę kasacyjną
191.	18.10.2013 r. I OSK 129/13	DOLiS/DEC-1081/11/63114, 63126	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 18.10.2012 r., II SA/Wa 692/12 w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - uchylenie zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania przez WSA w Warszawie
192.	18.10.2013 r.	DOLiS/DEC-	Skarga kasacyjna od wyroku	Wyrok NSA - uchylenie

	I OSK 1487/12	852/11/48406, 48408	WSA w Warszawie z dnia 13.03.2012 r., II SA/Wa 2558/11 w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	zaskarżonego wyroku i przekazanie sprawy do ponownego rozpoznania przez WSA w Warszawie
193.	22.10.2013 r. II SA/Wa 1249/13	DOLiS/DEC-464/13/24777, 24790	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
194.	22.10.2013 r. I OZ 988/13	DOLiS/DEC-314/13/17450, 17451,17492, 17457	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA – oddalenie zażalenia na zarządzenie WSA w Warszawie z dnia 6.08.2013 r., II SA/Wa 976/13 o pozostawieniu bez rozpoznania wniosku o przyznanie prawa pomocy w zakresie częściowym, obejmującym zwolnienie od kosztów sądowych
195.	22.10.2013 r. II SA/Wa 2296/12	DOLiS/POST-315/12/53547	Skarga na postanowienie o odmowie wszczęcia postępowania	Postanowienie WSA - odrzucenie zażalenia na postanowienie WSA w Warszawie z dnia 17.06.2013 r., II SA/Wa 2296/12
196.	24.10.2013 r. II SA/Wa 1465/13	DOLiS/DEC-176/09/8289, 8290	Skarga o wznowienie postępowania sądowego w sprawie II SA/Wa 710/09	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
197.	24.10.2013 r. I OSK 2496/13	DOLiS/DEC-1097/12/69181, 69183	Skarga na decyzję w przedmiocie nakazu udostępnienia danych	Postanowienie NSA – wstrzymanie wykonania zaskarżonej decyzji
198.	25.10.2013 r. II SA/Wa 605/13	DOLiS/DEC-53/13/3763,3766, 3773	Skarga na decyzję w przedmiocie nakazu udostępnienia danych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
199.	25.10.2013 r. II SA/Wa 998/13	DOLiS/DEC-377/13/20496, 20509	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
200.	28.10.2013 r. II SA/Wa 815/13	DOLiS/DEC-263/13/13825, 13830,13832	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 17.07.2013 r., II SA/Wa 815/13 w sprawie ze skargi na decyzję w przedmiocie odmowy uwzględnienia wniosku dotyczącego nieprawidłowości w procesie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi kasacyjnej
201.	28.10.2013 r. II SA 597/13	DOLiS/DEC-4/13/138,140	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
202.	29.10.2013 r. II SA/Wa 976/13	DOLiS/DEC-314/13/17450, 17451,17452, 17457	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
203.	31.10.2013 r. II SAB/Wa 486/13	DOLiS-440-43/13	Skarga na bezczynność GIODO w przedmiocie rozpoznania wniosku o przetwarzanie danych osobowych	Postanowienie WSA – odrzucenie skargi

204.	31.10.2013 r. II SAB 381/13	DOLiS/DEC-035-4067/12	Skarga na bezczynność GIODO w przedmiocie rozpoznania wniosku	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
205.	05.11.2013 r. II SA/Wa 624/13	DOLiS/DEC-46/13/3458,3459, 3463	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
206.	06.11.2013 r. II SA/Wa 1590/12	DOLiS/DEC-577/12/39478, 39479,39480	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
207.	06.11.2013 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820, 43822	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika
208.	07.11.2013 r. II SA/Wa 975/13	DOLiS/POST-78/13/17056, 17061	Skarga na postanowienie w przedmiocie stwierdzenia niedopuszczalności do wniesienia wniosku o ponowne rozpatrzenie sprawy	Postanowienie WSA – uchylenie zaskarżonego postanowienia
209.	07.11.2013 r. II SA/Wa 450/13	DOLiS/DEC-55/13/3819,3823, 3824,3828,3840	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
210.	08.11.2013 r. II SA/Wa 586/13	DOLiS/DEC-83/13	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
211.	08.11.2013 r. II SA/Wa 1264/13	DOLiS/DEC-495/13/26847, 26859,26861	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
212.	12.11.2013 r. II SA/Wa 1333/13	DOLiS/DEC-598/13/34106, 34107,34108	Skarga na decyzję w przedmiocie przekazania danych osobowych	Postanowienie WSA – odrzucenie skargi
213.	14.11.2013 r. II SA/Wa 1582/11	DOLiS/DEC-450/11/26448, 26449	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie ustanowienia pełnomocnika
214.	19.11.2013 r. II SAB/Wa 445/13	DOLiS-440-169/13	Skarga na przewlekłe prowadzenie postępowania przez GIODO w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż przewlekłość postępowania nie miała miejsca z rażącym naruszeniem prawa, w pozostałym zakresie umorzenie postępowania
215.	19.11.2013 r. II SA/Wa 1241/13	DOLiS/DEC-494/13/26812, 26814	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
216.	20.11.2013 r. II SA/Wa 2008/13	DOLiS/DEC-841/13/50817, 50819,50820, 50824,50829, 50833	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
217.	22.11.2013 r. II SAB/Wa 403/13	DOLiS-440-1530/12	Skarga na bezczynność GIODO w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż bezczynność nie miała miejsca z rażącym naruszeniem prawa, w pozostałym zakresie umorzono postępowanie
218.	26.11.2013 r. II SA/Wa 1308/13	DOLiS/DEC-502/13/27210, 27216	Skarga na decyzję w przedmiocie umorzenia postępowania	Wyrok WSA – oddalenie skargi

			administracyjnego	
219.	28.11.2013 r. II SAB/Wa 402/13	DOLiS-440-857/12	Skarga na bezczynność GIODO w przedmiocie rozpoznania wniosku dotyczącego przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż bezczynność nie miała miejsca z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie
220.	28.11.2013 r. II SA/Wa 1988/13	DOLiS/DEC-1097/12/69181, 69183	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie zwolnienia od kosztów sądowych
221.	29.11.2013 r. II SA/Wa 1506/13	DOLiS/POST-147/13/34930	Skarga na postanowienie w przedmiocie zwrotu pisma z uwagi na nieuiszczenie opłaty skarbowej	Postanowienie WSA – odmowa przyznania prawa pomocy w zakresie zwolnienia od uiszczenia wpisu sądowego i ustanowienia pełnomocnika
222.	02.12.2013 r. II SA/Wa 1400/13	DOLiS/DEC-592/13/33390, 33395	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
223.	02.12.2013 r. II SA/Wa 1194/13	DOLiS/POST-127/13/29233, 29244	Skarga na postanowienie w przedmiocie stwierdzania uchybienia terminu do złożenia wniosku o ponowne rozpatrzenie sprawy	Wyrok WSA – uchylenie zaskarżonego postanowienie i określenie, że nie podlega wykonaniu w całości
224.	03.12.2013 r. II SA/Wa 747/13	DOLiS/DEC-156/13/9453, 9462,9467	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości
225.	04.12.2013 r. II SAB/Wa 343/13	GI-DS-430/614/02	Skarga na bezczynność GIODO w przedmiocie rozpatrzenia wniosku	Wyrok WSA – oddalenie skargi
226.	05.12.2013 r. II SA/Wa 1557/13	DOLiS/DEC-127/13/29233, 29244	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
227.	05.12.2013 r. II SA/Wa 1135/13	DOLiS/DEC-443/13/23990, 23992,23994, 23995,23997, 23999	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
228.	06.12.2013 r. II SA/Wa 1134/13	DOLiS/POST-112/13/25244	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania w sprawie ochrony danych osobowych	Wyrok WSA – uchylenie zaskarżonego postanowienia i poprzedzającego go postanowienia oraz stwierdzenie, że nie podlegają wykonaniu w całości
229.	06.12.2013 r. II SA/Wa 626/13	DOLiS/DEC-48/13/3701,3702, 3703	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
230.	09.12.2013 r. II SA/Wa 1568/13	DOLiS/DEC-609/13/ 35406/35422/35430/35434/35443/35448/35451/35455/ 35458/35461/ 35465/35470	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
231.	09.12.2013 r. II SA/Wa 1367/13	DOLiS/DEC-506/13/27373, 27376,27378	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Wyrok WSA – oddalenie skargi

			o zabezpieczenie danych osobowych	
232.	12.12.2013 r. II SA/Wa 814/13	DOLiS/DEC-82/13/5890,5901	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na nieprawidłowości w procesie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej ją decyzji oraz stwierdzenie, że zaskarżona decyzja nie podlega wykonaniu w całości

Załącznik nr 4

Informacje przekazane przez organy ścigania w sprawach zawiadomień o popełnieniu przestępstwa skierowanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2013 r.

Informacja	**Rok 2011**	**Rok 2012**	**Rok 2013**
Umorzenie dochodzenia	14	9	5
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	-	-	-
Umorzenie dochodzenia i odmowa podjęcia go na nowo	1	-	-
Wszczęcie dochodzenia	10	-	2
Odmowa wszczęcia dochodzenia	3	3	3
Wszczęcie śledztwa i jego umorzenie	-	-	2
Zawieszenie dochodzenia	1	-	-
Skierowanie sprawy do sądu	1	-	-
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	1	1	-
Brak informacji	1	1	4

Załącznik nr 5

Wykaz szkoleń przeprowadzonych przez GIODO w 2013 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	28.01.2013	Warszawa	Komenda Główna Policji – szkolenie dla trenerów użytkowników KSI
2.	30.01.2013	Warszawa	Komenda Główna Policji – szkolenie dla trenerów użytkowników KSI
3.	04.02.2013	Warszawa	Komenda Główna Policji – szkolenie dla trenerów użytkowników KSI
4.	05.02.2013	Kraków	Małopolski Urząd Wojewódzki w Krakowie
5.	06.02.2013	Warszawa	Komenda Główna Policji – szkolenie dla trenerów użytkowników KSI
6.	07.02.2013	Warszawa	Ministerstwo Spraw Zagranicznych
7.	13.02.2013	Warszawa	Krajowa Rada Spółdzielcza
8.	19.02.2013	Warszawa	Kancelaria Sejmu
9.	20.02.2013	Warszawa	Kancelaria Sejmu
10.	20.02.2013	Warszawa	Agencja Rynku Rolnego
11.	21.02.2013	Warszawa	Kancelaria Sejmu
12.	22.02.2013	Warszawa	Kancelaria Sejmu
13.	26.02.2013	Warszawa	Sąd Okręgowy w Warszawie
14.	26.02.2013	Warszawa	Komenda Główna Państwowej Straży Pożarnej
15.	05.03.2013	Warszawa	Główny Inspektorat Weterynarii
16.	11.03.2013	Warszawa	Komenda Główna Państwowej Straży Pożarnej
17.	20.03.2013	Warszawa	Mazowiecka Jednostka Wdrażania Programów Unijnych
18.	22.03.2013	Warszawa	Kancelaria Sejmu
19.	25.03.2013	Warszawa	Ministerstwo Administracji i Cyfryzacji – szkolenie dla przedstawicieli 16 urzędów wojewódzkich
20.	28.03.2013	Wrocław	Urząd Marszałkowski Województwa Dolnośląskiego
21.	02.04.2013	Warszawa	Ministerstwo Spraw Zagranicznych
22.	04.04.2013	Warszawa	Sąd Okręgowy w Warszawie
23.	15.04.2013	Warszawa	Ministerstwo Administracji i Cyfryzacji – szkolenie dla wojewodów
24.	17.04.2013	Warszawa	Mazowiecki Oddział Żandarmerii Wojskowej oraz jednostek podległych
25.	19.04.2013	Radom	Komenda Wojewódzka Policji w Radomiu, Komenda Stołeczna Policji w Warszawie, komendy miejskie i powiatowe garnizonu mazowieckiego i In.
26.	22.04.2013	Radom	Kuratorium Oświaty w Warszawie Delegatura Radom

27.	06.05.2013	Poznań	Urząd Miasta Poznań
28.	06.05.2013	Poznań	Wielkopolska Izba Przemysłowa – sejmik gospodarczy
29.	06.05.2013	Poznań	Urząd Marszałkowski Województwa Wielkopolskiego
30.	07.05.2013	Poznań	Urząd Marszałkowski Województwa Wielkopolskiego – przedstawiciele urzędów marszałkowskich oraz jednostek podległych
31.	07.05.2013	Poznań	Wielkopolski Urząd Wojewódzki w Poznaniu
32.	13.05.2013	Warszawa	Inspektorat Wojskowej Służby Zdrowia
33.	13.05.2013	Warszawa	Ministerstwo Sprawiedliwości
34.	17.05.2013	Zielona Góra	Urząd Marszałkowski Województwa Lubuskiego
35.	22.05.2013	Warszawa	Polska Agencja Rozwoju Przedsiębiorczości
36.	10.06.2013	Warszawa	Rządowe Centrum Legislacji
37.	17.06.2013	Warszawa	Ministerstwo Spraw Zagranicznych
38.	21.06.2013	Warszawa	Ośrodek Rozwoju Edukacji
39.	21.06.2013	Warszawa	Ministerstwo Finansów
40.	24.06.2013	Warszawa	Ministerstwo Finansów
41.	12.07.2013	Warszawa	Ministerstwo Spraw Zagranicznych
42.	02.09.2013	Warszawa	Teatr Roma
43.	06.09.2013	Warszawa	Naczelna Izba Lekarska
44.	09.09.2013	Warszawa	Akademia Obrony Narodowej
45.	10.09.2013	Warszawa	Ministerstwo Spraw Zagranicznych
46.	10.10.2013	Warszawa	Ministerstwo Pracy i Polityki Społecznej
47.	11.10.2013	Warszawa	Okręgowa Izba Radców Prawnych w Kielcach
48.	15.10.2013	Warszawa	Ministerstwo Spraw Zagranicznych
49.	15.10.2013	Warszawa	Agencja Rozwoju Mazowsza S.A.
50.	17.10.2013	Poznań	Wielkopolska Izba Rzemieślnicza w Poznaniu
51.	24.10.2013	Warszawa	Ministerstwo Sprawiedliwości
52.	24-25.10.2013	Warszawa	Przedstawiciele szkół i placówek doskonalenia zawodowego nauczycieli w ramach IV ogólnopolskiego programu edukacyjnego „Twoje dane - twoja sprawa (…)"
53.	05.11.2013	Warszawa	Ministerstwo Środowiska
54.	22.11.2013	Warszawa	Okręgowa Izba Radców Prawnych we Wrocławiu
55.	25.11.2013	Gdańsk	Okręgowa Izba Radców Prawnych w Gdańsku
56.	28.11.2013	Warszawa	Urząd Miasta st. Warszawa – przedstawiciele Zakładów Opieki Zdrowotnej
57.	09.12.2013	Kraków	Okręgowa Izba Radców Prawnych w Krakowie
58.	10.12.2013	Warszawa	Biuro Zarządzania Ryzykiem i Zgodności, Poczta Polska S.A.
59.	12.12.2013	Warszawa	Warszawski Uniwersytet Medyczny
60.	12.12.2013	Warszawa	Wojskowa Akademia Techniczna

Załącznik nr 6

Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych w 2013 r.

1. III edycja Konkurs „Bezpieczny eSklep". Organizator: Instytut Logistyki i Magazynowania. Poznań, styczeń – marzec 2013 r.
2. Łódzki Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji", 4-5 lutego 2013 r.
3. Podlaski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji", 20 lutego 2013 r.
4. Ogólnopolski Konkurs „Prawo a Nowe Technologie". Organizator: Studenckie Koło Naukowe – Blok Prawa Komputerowego. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Wrocław, marzec – kwiecień 2013 r.
5. VI Konferencja SEMAFOR (Security, Management, Audit, Forum). Organizator: magazyn Computerworld oraz Stowarzyszenia: ISSA Polska i ISSACA Warsaw Chapter. Warszawa, 5-6 marca 2013 r.
6. XIV Prawnicze Targi Pracy. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland. Warszawa, 6 marca 2013 r.
7. Konferencja naukowa „Ataki Sieciowe". Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii przy Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu. Toruń, 18 marca 2013 r.
8. Międzynarodowa Konferencja *Safety and Security* pt. „Nowoczesne technologie, systemy i rozwiązania organizacyjne dla bezpieczeństwa informacji i danych osobowych". Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Bielsko-Biała, 20-22 marca 2013 r.
9. Seminarium nt. ochrony danych osobowych w nowych technologiach. Organizator: Fundacja Bezpieczna Cyberprzestrzeń. Warszawa, 21 marca 2013 r.
10. Lubelski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji". Janów Lubelski, 21-22 marca 2013 r.
11. Konferencja „Dyrektor XXI wieku – mobilność, bezpieczeństwo, innowacyjność". Organizator: Firma Librus oraz Magazyn EduFakty – Uczę Nowocześnie. Mszczonów, 12-13 kwietnia 2013 r.
12. Warmińsko-Mazurski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji". Wilkasy k/Giżycka, 18-19 kwietnia 2013 r.

13. Kongres Regulacji Prawnych z Obszaru Zarządzania Wierzytelnościami. Organizator: Konferencja Przedsiębiorstw Finansowych w Polsce. Warszawa, 24 kwietnia 2013 r.

14. I Wiosenny Konwent Ochrony Danych i Informacji. Organizator: Forsafe. Łódź, 8 maja 2013 r.

15. Pomorski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji". Jurata, 20-21 maja 2013 r.

16. Konferencja Naukowa pt. „Dane medyczne – granice wykorzystywania i ochrona". Organizator: Podyplomowe Studium Ochrony Danych Osobowych na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 23 maja 2013 r.

17. Polsko-Niemiecka Konferencja pt. „Prawo do dostępu do informacji wobec organów władzy publicznej". Organizatorzy: Szkoła Prawa Niemieckiego na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, Wydział Nauk o Państwie i Prawie Uniwersytetu w Bonn oraz Niemiecka Fundacja Międzynarodowej Współpracy Prawnej. Warszawa, 24 maja 2013 r.

18. IX Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych poświęcony ochronie informacji i danych osobowych w przedsiębiorstwach i instytucjach, z uwzględnieniem aktualnych i planowanych zmian w przepisach prawa o ochronie danych osobowych oraz stosowania ich w praktyce. Organizatorzy: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego. Bielsko-Biała, 27-29 maja 2013 r.

19. II Międzynarodowa Konferencja Zarządzania Ciągłością Działania pt. „Zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów Państwa w obliczu dzisiejszych zagrożeń". Organizatorzy: Wyższa Szkoła Policji w Szczytnie oraz British Standards Institution Group Polska. Szczytno, 4-5 czerwca 2013 r.

20. VII Forum IAB Polska, poświęcone marketingowi w Internecie. Organizator: Związek Pracodawców Branży Internetowej IAB Polska. Warszawa, 5-6 czerwca 2013 r.

21. Małopolski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji", Krynica-Zdrój, 13-14 czerwca 2013 r.

22. Konferencja Naukowa „Komunikacja elektroniczna w administracji publicznej". Organizator: Wyższa Szkoła Informatyki i Zarządzania pod auspicjami Polskiej Akademii Nauk. Warszawa, PAN, 28 czerwca 2013 r.

23. Mazowiecki Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji". Grębiszew k/Mińska Mazowieckiego, 12-13 września 2013 r.

24. Konferencja „Pięć żywiołów. Systemy inteligentne w zarządzaniu kryzysowym i działaniach militarnych". Organizatorzy: Fundacja „Instytut Mikromakro", Ośrodek Badań nad Przyszłością Collegium Civitas, Stowarzyszenie Euro-Atlantyckie oraz Przemysłowy Instytut Automatyki i Pomiarów – PIAP. Warszawa, 30 września – 1 października 2013 r.

25. I Jesienny Konwent Ochrony Danych i Informacji. Organizator: Golden Floor Business Uniwersity Park w Łodzi. Łódź, 2 października 2013 r.

26. III Śląski Konwent Informatyków I Administracji Pt. „Podpis elektroniczny i inne wyzwania ICT przed przyszłą perspektywą finansową UE". Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Hucisko, 3-4 października 2013 r.

27. XV Forum Monitoringu Polskiego pn. „Aktualne aspekty prawno-normatywne oraz trendy techniczne monitoringu bezpieczeństwa obiektów". Organizator: Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem POLALARM. Pułtusk, 3-4 października 2013 r.

28. VI Kongres Warsaw International Media Summit oraz towarzysząca mu VI Konferencja „Zmiany w regulacjach i prawie Świata Telekomunikacji i Mediów". Organizator MM Conferences S.A. Warszawa, 9-10 października 2013 r.

29. XVII Konferencja na temat bezpieczeństwa teleinformatycznego „SECURE 2013". Organizatorzy: Naukowa i Akademicka Sieć Komputerowa (NASK) i CERT Polska. Warszawa, 9-10 października 2013 r.

30. VI Konwent Informatyków i Administracji Pomorza i Kujaw pt. „Cyfrowa Polska nowoczesny region. Realizacja, wdrożenia i przyszłość projektów IT/CT". Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Ciechocinek, 24-25 października 2013 r.

31. Wielkopolski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji", 24-25 października 2013 r.

32. V Kongres „Healthcare IT Trends 2013". Organizatorzy: Healthcare Management Magazine oraz Akademia Wiedza i Praktyka. Warszawa, 29 października 2013 r.

33. VII Zachodniopomorski Konwent Informatyków i Administracji pt. „Cyfrowa Polska nowoczesny region. Realizacja, wdrożenia i przyszłość projektów IT/CT". Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Dwór Pomorski – Luboradza, 14-15 listopada 2013 r.

34. Dolnośląski Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji". Jugowice, 21-22 listopada 2013 r.

35. V Ogólnopolska Konferencja Dyrektorów i Pracowników Administracyjnych Szkół. Organizator: Instytut Raabe. Warszawa, 22 listopada 2013 r.

36. Konferencja „ATAK i OBRONA 2013". DDoS / APT". Organizator: Fundacja Bezpieczna Cyberprzestrzeń. Warszawa, 26 listopada 2013 r.

37. XII Konferencja „Systemy Informatyczne w Energetyce". Organizator: Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej. Wisła, 26-29 listopada 2013 r.

38. Międzynarodowa Konferencja Naukowa p.t. „Wyzwania dla rynku ubezpieczeń komunikacyjnych". Organizator: Instytut Ekonometrii Szkoły Głównej Handlowej,

Stowarzyszenie PRO MOTOR, Zakład Finansów i Zarządzania Ryzykiem Politechniki Warszawskiej, Zakład Ubezpieczeń i Rynków Kapitałowych Wydziału Zarządzania Uniwersytetu Warszawskiego. Warszawa, 4 grudnia 2013 r.

39. VI Międzynarodowa Konferencja „Central European Electronic Card Warsaw 2013. Organizator: Medien Service. Warszawa, 4-5 grudnia 2013 r.

40. III Lubuski Konwent Informatyków i Administracji pt. „Cyfrowa Polska nowoczesny region. Realizacja, wdrożenia i przyszłość projektów IT/CT". Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Gronów, 5-6 grudnia 2013 r.

41. Podkarpacki Konwent Informatyków, Organizator: Redakcja Miesięcznika „IT w Administracji", 12-13 grudnia 2013 r.

42. Portal informacyjny „Bezpieczna Chmura", którego twórcą i realizatorem jest polski oddział Stowarzyszenia Cloud Security Alliance Polska.

Załącznik nr 7

Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2013 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty

l.p.	Data	Konferencja/Seminarium	Miejsce
1.	18.01.2013	Wykład otwarty Generalnego Inspektora Ochrony Danych Osobowych podczas inauguracji studiów podyplomowych w SGH. Organizator: Szkoła Główna Handlowa	Warszawa
2.	22.01.2013	II Dzień Ochrony Informacji Niejawnych połączony z Dniem Otwartym nt. ochrony informacji niejawnych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych	Dąbrowa Górnicza
3.	28.01.2013	VII Dzień Ochrony Danych Osobowych. Konferencja „Dane osobowe w ochronie zdrowia i w badaniach klinicznych". Organizator: GIODO	Warszawa
4.	05.02.2013	II Łódzki Konwent Informatyków. Organizator: Redakcja Miesięcznika „IT w Administracji"	Spała
5.	12.02.2013	Spotkanie GIODO z prezesami sądów, dyrektorami, sędziami i pracownikami sądów apelacji wrocławskiej. Organizator: Sąd Apelacyjny we Wrocławiu	Wrocław
6.	13.02.2013	2. Kongres Wolności w Internecie. Organizator: Ministerstwo Administracji i Cyfryzacji	Warszawa
7.	13.02.2013	Seminarium „Kierunki zmian w europejskim prawie dotyczącym ochrony danych osobowych i ich wpływ na sektor bankowy". Organizator: Związek Banków Polskich	Warszawa
8.	19.02.2013	Konferencja nt. praktycznych aspektów funkcjonowania ustawy deweloperskiej. Organizator: Wydawnictwo Komentarzy Praktycznych	Warszawa
9.	20.02.2013	XII edycja seminarium z cyklu „Teleinformatyka w przedsiębiorstwach sieciowych", pt. „Rozwój technologii do wdrażania *smart metering/grid* w przedsiębiorstwach sieciowych". Organizator: Centrum Promocji Informatyki	Warszawa
10.	20-21.02.2013	Seminarium „Accountability Phase V. The Essentials Elements in Distributed Environments. Organizator: GIODO oraz Centre for Information Policy Leadership	Warszawa
11.	22.02.2012	Międzynarodowa Konferencja 2013 ePSI pt. „Gotcha! – getting everyone on bard". Organizator: ePSI Platform i Centrum Cyfrowe	Warszawa
12.	22.02.2013	Konferencja nt. ochrony danych osobowych i wizerunku ofiar przestępstw. Organizator: Prokuratura Generalna	Warszawa
13.	25.02.2013	Warsztaty na temat praktyk wdrożenia procedur FATCA w polskich instytucjach finansowych. Organizator: MMC Polska	Warszawa
14.	26.02.2013	Konferencja „Nadużycia we wnioskach kredytowych". Organizator: SmithNovak, s.r.o. Praga	Warszawa
15.	27.02.2013	IV edycja Forum Prawa Nowych Technologii „Prawo komunikacji elektronicznej w praktyce gospodarki i administracji". Organizator: Polskie Centrum Informatyki	Warszawa
16.	28.02.2013	IV Forum „Corporate Legal Counsel 2013" – Forum	Warszawa

		Dyrektorów Prawnych. Organizator: Blue Business Media	
17.	01.03.2013	Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z Dyrektor Generalną ds. Sprawiedliwości Komisji Europejskiej Françoise Le Bail.	Warszawa
18.	01.03-30.04.2013	III edycja Konkursu z zakresu ochrony danych osobowych wykorzystywanych do profilowania klientów dla celów działań marketingowych. Organizator: Generalny Inspektor Ochrony Danych Osobowych, partner merytoryczny: PricewaterhouseCoopers Legal Szurmińska-Jaworska spółka komandytowa	Warszawa
19.	5-6.03.2013	VI Konferencja SEMAFOR (Security, Management, Audit, Forum). Organizator: Magazyn Computerworld oraz Stowarzyszenia: ISSA Polska i ISSACA Warsaw Charter	Warszawa
20.	14.03.2013	Polski Kongres Prawa Farmaceutycznego i Ochrony Zdrowia 2013 *„Allerhand summie: Pharma & Heath”*. Organizator: Fundacja Instytut Allerhanda	Warszawa
21.	18.03.2013	Konferencja Naukowa „Ataki Sieciowe”. Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii przy Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu	Toruń
22.	19.03.2013	Omówienie założeń projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływie tych danych – podczas spotkania w siedzibie Krajowej Izby Gospodarczej	Warszawa
23.	20.03.2013	Debata „Prywatność w nowych technologiach”. Organizator: Fundacja Bezpieczna Cyberprzestrzeń oraz Koło Naukowe CyberLaw Uniwersytetu Warszawskiego	Warszawa
24.	20.03.2013	6. Konferencja TeraForum pod hasłem”Informatyka ad acta?” związanej z obchodami 20-lecia Polskiej Izby Informatyki i Telekomunikacji. Organizator: Polska Izba Informatyki i Telekomunikacji	Warszawa
25.	21.03.2013	Forum „Informatyka w bankowości. Trendy informatyczne w bankowości spółdzielczej”. Organizator: Centrum Promocji Informatyki	Warszawa
26.	26.03.2013	Międzynarodowa Konferencja „Operator Informacji Pomiarowych – pozycja na rynku (kluczowe problemy prawne i biznesowe). Organizator: Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej oraz AEEC Associated European Energy Consultans	Warszawa
27.	27.03.2013	Seminarium “*Legal transplants in IT influenced Word”*. Organizatorzy: Komisja Fulbrighta wspólnie z IIT/Chicago-Kent College of Law, Uniwersytetem Gdańskim, Uniwersytetem Wrocławskim oraz Wyższą Szkołą Handlu i Prawa im. Ryszarda Łazarskiego w Warszawie	Warszawa
28.	27-28.03.2013	XIII Sympozjum Świata Telekomunikacji i Mediów – Rynek Telekomunikacyjny i Media. Organizator: MMC Polska	Warszawa
29.	05.04.2013	XII Krajowa Konferencja Szkoleniowa TIP „Postępy w chorobach wewnętrznych – INTERNA 2013”. Organizator: specjalistyczny portal internetowy Medycyna Praktyczna oraz Towarzystwo Internistów Polskich	Warszawa
30.	12.04.2013	Konferencja „Dyrektor XXI wieku – mobilność, bezpieczeństwo, innowacyjność”. Organizator: Firma Librus oraz Magazyn EduFakty – Uczę Nowocześnie	Mszczonów
31.	16.04.2013	Wspólne posiedzenie Sejmowej i Senackiej Komisji Sprawiedliwości w formie Konferencji Naukowej pt. „Reforma	Warszawa

		unijnego prawa ochrony danych osobowych". Organizatorzy: Senacka Komisja Praw Człowieka, Sprawiedliwości i Petycji oraz Komisja Sprawiedliwości i Praw Człowieka Sejmu RP	
32.	17.04.2013	Warsztaty nt. „Obrotu wierzytelnościami na polskim rynku". Organizator: Business Media Solutions	Warszawa
33.	17.04.2013	II Konferencja z cyklu „Normalizacja w szkole". Organizator: Polski Komitet Normalizacyjny	Warszawa
34.	18-19.04.2013	Warmińsko-Mazurski Konwent Informatyków. Organizator: czasopismo „IT w Administracji"	Wilkasy k/Giżycka
35.	22.04.2013	Konferencja „Monitoring wizyjny w miejscach pozbawienia wolności". Organizator: Rzecznik Praw Obywatelskich	Warszawa
36.	22.04.2013	III Konferencja Naukowa „Cyberprzestępczość i ochrona informacji" pn. „Ochrona prywatności i własności intelektualnej w Internecie". Organizatorzy: Wyższa Szkoła Menedżerska oraz Polskie Towarzystwo Informatyczne	Warszawa
37.	22-23.04.2013	Międzynarodowa Konferencja Naukowa z okazji 60. rocznicy wejścia w życie Europejskiej Konwencji Praw Człowieka „Uniwersalny i regionalny wymiar ochrony praw człowieka. Nowe wyzwania – nowe rozwiązania". Organizatorzy: Instytut Ekonomii i Administracji Uniwersytetu Jana Kochanowskiego w Kielcach oraz Komisja Sprawiedliwości i Praw Człowieka Sejmu RP	Warszawa
38.	24.04.2013	Kongres Regulacji Prawnych z Obszaru Zarządzania Wierzytelnościami. Organizator: Konferencja Przedsiębiorstw Finansowych w Polsce	Warszawa
39.	25.04.2013	VII Międzynarodowa Konferencja Naukowa „Internet w Społeczeństwie Informacyjnym". Organizator: Wyższa Szkoła Biznesu w Dąbrowie Górniczej oraz Polska Izba Gospodarcza Zaawansowanych Technologii w Warszawie	Dąbrowa Górnicza
40.	26.04.2013	Dzień Ochrony Danych Osobowych w Banku BPH. Organizator: Bank BPH	Warszawa
41.	27.04.2013	Konferencja pt. „Prawa dziecka". Organizator: Naczelna Rada Adwokacka	Gdańsk
42.	06.05.2013	Konferencja „Bezpieczeństwo publiczne i rozwój. Nowe technologie w przestrzeni publicznej przy wsparciu Unii Europejskiej. Organizatorzy: Prezydent Miasta Gliwice oraz Śląska Sieć Metropolitarna	Gliwice
43.	06-07.05.2013	XXI Spotkanie Klubu Informatyka Samorządowego	Puszczykowo k/Poznania
44.	07.05.2013	Konferencja pt. „Bezpieczeństwo sieci Smard Grid". Organizator: Polskie Towarzystwo Informatyczne	Warszawa
45.	07.05.2013	Konferencja Naukowa pt „Prawne i ekonomiczne aspekty przetwarzania danych osobowych w Unii Europejskiej" oraz Konferencja Szkoleniowa w Urzędzie Marszałkowskim Województwa Wielkopolskiego pt. „Problemy ochrony danych osobowych w urzędach marszałkowskich oraz nadzorowanych jednostkach organizacyjnych samorządu województwa", zorganizowane w ramach Dnia Otwartego Biura Generalnego Inspektora Ochrony Danych Osobowych w Poznaniu.	Poznań
46.	08.05.2013	1. Wiosenny Konwent Ochrony Danych i Informacji. Organizator: Forsafe	Łódź
47.	10.05.2013	Śniadanie GIODO z przedstawicielami firm obsługujących sektor biznesu. Organizator: Iron Mountain	Warszawa
48.	13.05.2013	Debata „Cyfrowa tożsamość – kim jesteśmy w Internecie i jak dzielimy się wiedzą o sobie" z udziałem Viviane Reding, wiceprzewodniczącej KE, Komisarz Sprawiedliwości, Praw	Warszawa

		Podstawowych i Obywatelstwa. Organizator: Ministerstwo Administracji i Cyfryzacji	
49.	20-21.05.2013	Pomorski Konwent Informatyków. Organizator: czasopismo "IT w Administracji"	Jurata
50.	22.05.2013	V Konferencja Naukowa „Bezpieczeństwo w Internecie. Internet – granice jawności". Organizatorzy: Uniwersytet Kardynała Stefana Wyszyńskiego, Naukowe Centrum Prawno-Informatyczne, Generalny Inspektor Ochrony Danych Osobowych	Warszawa
51.	23.05.2013	Konferencja Naukowa „Dane medyczne – granice wykorzystywania i ochrona". Organizator: Podyplomowe Studium Ochrony Danych Osobowych na Wydziale Prawa i Administracji UŁ	Łódź
52.	23.05.2013	XIV Forum ADO/ABI (administratorów danych osobowych i administratorów bezpieczeństwa informacji). Organizator: Centrum Promocji Informatyki	Warszawa
53.	24.05.2013	Seminarium Microsoftu poświęcone zastosowaniu modelu chmury w administracji publicznej, zorganizowane w siedzibie Polskiej Rady Biznesu	Warszawa
54.	27-29.05.2013	IX Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych poświęcony ochronie informacji i danych osobowych w przedsiębiorstwach i instytucjach, z uwzględnieniem aktualnych i planowanych zmian w przepisach prawa o ochronie danych osobowych oraz stosowania ich w praktyce. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego	Bielsko-Biała
55.	28-29.05.2013	XVI Konferencja pt. „Techniczne Aspekty Przestępczości Teleinformatycznej". Organizator: Wyższa Szkoła Policji w Szczytnie	Szczytno
56.	03.06.2013	Seminarium podsumowujące 3. edycję ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Organizator: Generalny Inspektor ochrony Danych Osobowych.	Warszawa
57.	06-07.06.2013	6. Międzynarodowa Konferencja MCSS 2013 "Multimedia Communications, Services & Security" zorganizowanej na Wydziale Telekomunikacji Akademii Górniczo Hutniczej w Krakowie	Kraków
58.	13.06.2013	Forum Sekretarzy Województwa Kujawsko-Pomorskiego. Organizator: Fundacja Rozwoju Demokracji Lokalnej – Kujawsko-Pomorskie Biuro FRDL	Białe Błota
59.	13.06.2013	Konferencja pt. „Ochrona danych osobowych w sektorze ubezpieczeń". Organizator: V Financial Conferences	Warszawa
60.	18.06.2013	59. edycja Seminarium „Akademia Prawa Komputerowego" pt. „Profilowanie w Internecie. Nadużywanie danych osobowych". Organizator: Centrum Promocji Informatyki	Warszawa
61.	20.06.2013	Konferencja „Płatności mobilne w drodze do wygody i bezpieczeństwa". Organizator: Medien Service	Warszawa
62.	24-25.06.2013	I Letnie Spotkania PTI. Organizator: Polskie Towarzystwo Informatyczne Oddział Górnośląski	Szczyrk
63.	26.06.2013	Debata „Prywatność i dane osobowe w inteligentnych sieciach energetycznych". Organizator: Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej	Warszawa
64.	28.06.2013	Konferencja Naukowa pt. „Komunikacja elektroniczna w administracji publicznej". Organizator: Wyższa Szkoła	Warszawa

		Informatyki i Zarządzania pod auspicjami Polskiej Akademii Nauk	
65.	11.09.2013	Konferencja pt. „Monitoring wizyjny w przestrzeni publicznej miasta – aspekty prawne, organizacyjne i techniczne”. Organizator: Urząd Miasta Poznań	Poznań
66.	16.09.2013	III Europejski Kongres Małych i Średnich Przedsiębiorstw. Organizator: Regionalna Izba Gospodarcza w Katowicach	Katowice
67.	17.09.2013	Konferencja „Wykorzystanie danych z rejestrów publicznych budowanych w ramach 7 Osi POIG”. Organizator: Władza Wdrażająca Programy Europejskie.	Warszawa
68.	18.09.2013	Ogólnopolska Konferencja Naukowo-Szkoleniowa „IT w zdrowiu – zmiany w sektorze zdrowia i prognoza 2014-2020”. Organizator: Śląska Sieć Metropolitarna	Gliwice
69.	19.09.2013	LXII edycja seminarium z cyklu Akademia Prawa Komputerowego pt. „Bezprawne treści w Internecie – analiza orzecznictwa polskich organów i sądów oraz TSUE”. Organizator: Centrum Promocji Informatyki	Warszawa
70.	23-26.09.2013	35. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności „Prywatność – przewodnik po zagmatwanym świecie”. Organizator: Generalny Inspektor Ochrony Danych Osobowych	Warszawa
71.	24.09.2013	Warsztaty w ramach projektu PHAEDRA	Warszawa
72.	27.09.2013	Spotkanie GIODO z przedstawicielami Urzędu Rzecznika Ochrony Prywatności Kanady	Warszawa
73.	02.10.2013	I Jesienny Konwent Ochrony Danych i Informacji. Organizator: Golden Floor Business Uniwersity Park w Łodzi	Łódź
74.	04.10.2013	XV Forum Monitoringu Polskiego pn. „Aktualne aspekty prawno-normatywne oraz trendy techniczne monitoringu bezpieczeństwa obiektów”. Organizator: Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem POLALARM	Pułtusk
75.	09-10.10.2013	XVII Konferencja dotycząca bezpieczeństwa teleinformatycznego pt. „SECURE 2013”. Organizatorzy: Naukowa i Akademicka Sieć Komputerowa (NASK) i CERT Polska	Warszawa
76.	09-10.10.2013	VI Kongres Warsaw International Media Summit oraz towarzysząca mu VI Konferencja „Zmiany w regulacjach i prawie Świata Telekomunikacji i Mediów”. Organizator MMC Polska	Warszawa
77.	11.10.2013	Konferencja Big Data. Organizator: Blue Business Media	Warszawa
78.	23.10.2013	Konferencja „Groupwork at SKNI”. Organizator: Studenckie Koło Naukowe Informatyki, Katedra Informatyki Gospodarczej Szkoły Głównej Handlowej	Warszawa
79.	23-25.10.2013	Ogólnopolski Kongres Rynku Pracy. Organizator: Stowarzyszenie „Edukacja – Praca – Przedsiębiorczość”	Częstochowa
80.	24.10.2013	63. edycja seminarium z cyklu Akademia Prawa Komputerowego, pt. „Najnowsze orzecznictwo sądowe z zakresu prawa nowych technologii komunikacyjnych – część I”. Organizator: Centrum Promocji Informatyki	Warszawa
81.	25.10.2013	Śniadanie Naukowe w Akademii im. Leona Koźmińskiego w ramach obchodów V edycji kampanii „Nie daj się okraść. Chroń swoją prywatność”. Organizator kampanii: firma Fellowes oraz Biuro Informacji Krajowej	Warszawa
82.	26.10.2013	Inauguracja Studiów Podyplomowych z zakresu bezpieczeństwa, zarządzania oraz informatyki w Wyższej Szkole Biznesu w Dąbrowie Górniczej	Dąbrowa Górnicza

83.	29.10.2013	V Konferencja „Healthcare IT Trends 2013”. Organizatorzy: Management Magazine oraz Akademia Wiedza i Praktyka	Warszawa
84.	5-6.11.2013	Konferencja Naukowa „Ochrona publicznych baz danych”. Organizator: Uniwersytet Kardynała Stefana Wyszyńskiego	Sobolewo
85.	13-14.11.2013	XVII Kongres ABI „Sieć Skutecznych Rozwiązań”. Organizator: ENSI	Chlewiska
86.	21-22.11.2013	Dolnośląski Konwent Informatyków. Organizator: Redakcja Miesięcznika IT w Administracji	Jugowice
87.	23.11.2013	Inauguracja II edycji studiów podyplomowych pn. „Ochrona Danych Osobowych i Informacji Prawnie Chronionych” w Wyższej Szkole Zarządzania i Bankowości w Krakowie	Kraków
88.	25-26.11.2013	CEE Fraud & Risk Conference „Crisis Management in Globalized Business Environment”. Organizator: IBBC Group	Warszawa
89.	26-29.11.2013	XII Konferencja „Systemy Informatyczne w Energetyce”. Organizator: Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej	Wisła
90.	04-05.12.2013	VI Konferencja Central European Electronic Card (CEEC) - Warsaw 2013. Organizator: Medien Service	Warszawa
91.	12.12.2013	Wykład dla studentów V roku Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego	Warszawa

Załącznik nr 8

Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2013 r. za granicą

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	07-08.01.2013	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
2.	08-10.01.2013	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
3.	13.01-09.02.2013	Program Partnerski LdV (projekt mobilności)	Trier-Trewir
4.	21-23.01.2013	Spotkanie w ramach projektu PHAEDRA (Vrije Universiteit Brussel)	Bruksela
5.	22.01.2013	Spotkanie GIODO z Rzecznikami Ochrony Danych Osobowych państw członkowskich UE, przedstawicielami PE, RE, KE, polskich ministerstw, urzędów centralnych, a także z przedstawicielami placówek dyplomatycznych w Brukseli oraz innych polskich i unijnych instytucji.	Bruksela
6.	23.01.2013	Okrągły Stół "EU Roundtable Discussion & White Paper launch. Organizator: Future of Privacy Forum.	Bruksela
7.	23-25.01.2013	„From 'Solidarity' to the Surveillance Society. Privacy Protection Dilemmas in Poland" - sesja podczas 6. Międzynarodowej Konferencji „Computers, Privacy and Data Protection (CPDP) 2013. Reloading Data Protection" . 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
8.	22-23.01.2013	Spotkanie w Komisji Europejskiej w sprawie Obchodów VII Europejskiego Dnia Ochrony Danych Osobowych	Bruksela
9.	29-30.01.2013	Spotkanie Podgrupy ds. Technologii	Bruksela
10.	08.02.2013	Posiedzenie Podgrupy ds. Biometrii & eGovernment Grupy Roboczej Art. 29	Bruksela
11.	10-23.02.2013	Program partnerski LdV (projekt mobilności)	Zagrzeb
12.	17-22.02.2013	Projekt partnerski LdV „Raising awareness of the data protection issues among the employees working in the EU"	Split
13.	20-21.02.2013	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy	Bruksela
14.	26-27.02.2013	89. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych	Bruksela
15.	03-23.03.2013	Program partnerski LdV (projekt mobilności)	Strasburg
16.	07.03.2013	3. Spotkanie Europejskiego Forum ds. e-fakturowania	Bruksela
17.	12-14.03.2013	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
18.	14.03.2014	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa	Bruksela

		(BTLE) Grupy Roboczej Art. 29	
19.	17.03-06.07.2013	Program partnerski LdV (projekt mobilności)	Bruksela
20.	18-19.03.2013	Wspólne Organy Nadzorcze ds. Europolu	Bruksela
21.	20-21.03.2013	Second meeting on notification of personal data breaches under the ePrivacy Directive and the Commission Regulation 611/2013; Meeting of the European Multi-Stakeholder Forum on Electronic invoicing	Bruksela
22.	20-21.03.2013	Międzynarodowa Konferencja „Online Privacy: Consenting to Your Future" zorganizowanej przez Universita ta Malta w ramach projektu "*CONSENT - Consumer sentiment regarding privacy on user generated content services in the digital economy*" w St. Julian's	Malta
23.	21-22.03.2013	Posiedzenie nie Podgrupy ds. Międzynarodowych Transferów. Spotkanie DG Home w sprawie misji Rosji.	Bruksela
24.	25-26.03.2013	Spotkanie Podgrupy ds. Technologii	Bruksela
25.	03.04.2013	Posiedzenie Podgrupy ds. Biometrii Grupy Roboczej Art. 29	Bruksela
26.	07-12.04.2013	Dialog wizowy z Rosją. Misja Komisji Europejskiej	Moskwa
27.	07-27.04.2013	Program partnerski LdV (projekt mobilności)	Strasburg
28.	09.04.2013	Seminarium "*The Right to be Forgotten*" zorganizowane przez Centre for European Legal Studies (CELS) na Wydziale Prawa Uniwersytetu w Cambridge	Cambridge
29.	10-12.04.2013	XV Konferencja Rzeczników Ochrony Prywatności Państw Europy Środkowej i Wschodniej	Belgrad
30.	10-12.04.2013	Posiedzenia grup: VIS/Eurodac – Europejski Zautomatyzowany System Rozpoznawania Odcisków Palców	Bruksela
31.	15-16.04.2013	53. Posiedzenie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska)	Praga
32.	16-17.04.2013	90. posiedzenie Grupy Roboczej Art. 29	Bruksela
33.	24-25.04.2013	Międzynarodowa Konferencja „Data Protection Intensive". Organizator: The International Association of Privacy Professionals	Londyn
34.	30.04.2013	Posiedzenie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions)	Bruksela
35.	13-17.05.2013	Międzynarodowa Konferencja „European Identity & Cloud Conference 2013". Organizator: KuppingerCole	Monachium
36.	16-17.05.2013	Wiosenna Konferencja Rzeczników Ochrony Danych 2013 „Ochrona prywatności i związane z nią wyzwania"	Lizbona
37.	21-22.05.2013	Spotkanie Podgrupy ds. Technologii	Bruksela
38.	23.05.2013	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
39.	29-30.05.2013	TAIEX Workshop on Civil & Criminal Liability for violating the right to personal data protection	Skopje
40.	02-29.06.2013	Wymiana doświadczeń w ramach projektu mobilności LdV	Ateny
41.	05-06.06.2013	91. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych	Bruksela
42.	10-11.06.2013	Posiedzenie Wspólnego Organu Nadzorczego nad Europolem	Bruksela
43.	10-11.06.2013	Posiedzenie Grypy Koordynującej Nadzór nad VIS i Eurodac	Bruksela
44.	25.06.2013	Spotkanie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions) Grupy Roboczej Art. 29	Bruksela
45.	03-04.07.2013	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
46.	21-24.07.2013	Projekt partnerski LdV „Raising awareness of the data protection issues among the employees working in the EU"	Sofia
47.	22-23.07.2013	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji	Bruksela

		i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	
48.	19-21.08.2013	Spotkanie z przewodniczącym regionalnego organu ochrony danych w Berlinie oraz z niemieckimi posłami do Parlamentu Europejskiego	Berlin
49.	09-10.09.2012	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX)	Bruksela
50.	01-03.09.2013	54. Spotkanie Międzynarodowej Grupy ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska)	Berlin
51.	04-05.09.2013	Spotkanie Podgrupy ds. Technologii	Ispra
52.	17.09.2013	4th Annual European Data Protection & Privacy Conference	Bruksela
53.	18.09.2013	Spotkanie Podgrupy ds. Prywatności (ePrivacy) Grupy Roboczej Art. 29. Organizator: Komisja Europejska, DG Connect.	Bruksela
54.	18.09.2013	Spotkanie Podgrupy ds. Technologii	Bruksela
55.	19.09.2013	Spotkanie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions) Grupy Roboczej Art. 29	Bruksela
56.	30.09-3.10.2013	Posiedzenie Grupy Roboczej Art. 29, E-Invoicing	Bruksela
57.	01-03.10.2013	XXV warsztaty rozpatrywania spraw. Organizator: Agencja Ochrony Danych Osobowych w Bośni i Hercegowinie	Sarajewo
58.	02-03.10.2013	92. Posiedzenie Grupy Roboczej Art. 29	Bruksela
59.	08-10.10.2013	Posiedzenie Wspólnego Organu Nadzorczego nad Europolem	Bruksela
60.	15-18.10.2013	30**.** Posiedzenie Plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD)	Strasburg
61.	16-17.10.2013	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
62.	21-28.10.2013	Kontrola Wizowego Systemu Informacyjnego (VIS)	Tel Aviv
63.	05-06.11.2013	Spotkanie Podgrupy ds. Technologii	Bruksela
64.	05-08.11.2013	IV International Conference „International cooperation as safeguarding of privacy in every country". Organizator: Rosyjski Urząd ds. Ochrony Danych.	Moskwa
65.	13-15.11.2013	Training Event 2013, BCR	Bonn
66.	13-16.11.2013	Projekt partnerski LdV „Raising awareness of the data protection issues among the employees working in the EU"	Praga
67.	02-04.12.2013	93. posiedzenie Grupy Roboczej Art. 29	Bruksela
68.	09-11.12.2013	Spotkanie JSB Europol i JSB Customs	Bruksela
69.	10-12.12.2013	IAPP Europe Data Protection Congress	Bruksela