SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja

Druk nr 116

Warszawa, 15 grudnia 2015 r.

Panie i Panowie Posłowie
na Sejm
Rzeczypospolitej Polskiej

Uprzejmie przekazuję przedstawiony przez Generalnego Inspektora Ochrony Danych Osobowych w dniu 14 października 2015 r. dokument

- „Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2014”.

MARSZAŁEK SEJMU

(-)Marek Kuchciński



SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VII kadencja
Generalny Inspektor Ochrony Danych Osobowych

Druk nr 4003

Warszawa, 13 października 2015 r.

Pani
Małgorzata Kidawa-Błońska
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek,

pragnę złożyć na Pani ręce

- Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2014

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.

Z poważaniem

(-) dr Edyta Bielak-Jomaa

Generalny Inspektor
Ochrony Danych Osobowych

SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2014

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182 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 2014 r. do 31 grudnia 2014 r.

SPIS TREŚCI

Spis treści

Wprowadzenie **5**

Część I. Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych. **6**

1. Informacje ogólne. 6
2. Reforma ochrony danych osobowych w Unii Europejskiej. 10
3. Biuro Generalnego Inspektora Ochrony Danych Osobowych. 13
3.1. Struktura organizacyjna. 13
3.2. Pracownicy Biura GIODO. 15
3.3. Budżet Generalnego Inspektora Ochrony Danych Osobowych za 2014 r. 15

Część II. Stan wiedzy i przestrzegania przepisów o ochronie danych osobowych. **16**

1. Informacje ogólne. 16
2. Kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. 19
2.1. Czynności kontrolne. 19
2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach. 20
2.3. Systemy informatyczne służące do przetwarzania danych osobowych. 56
2.4. Wyniki kontroli w zakresie obowiązków formalnych i organizacyjnych. 56
2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych. 59
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych. 65
3.1. Wydawanie decyzji. 65
3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa. 66
3.3. Rozpatrywanie skarg. 68
3.3.1. Administracja publiczna. 70
3.3.2. Bezpieczeństwo publiczne. 73
3.3.3. Sądy, prokuratura, komornicy. 75
3.3.4. Organizacje społeczne. 77
3.3.5. Banki i inne instytucje finansowe. 78
3.3.6. Internet. 80

3.3.7. Marketing. 82
3.3.8. Mieszkalnictwo. 83
3.3.9. Oświata i szkolnictwo wyższe. 84
3.3.10. Służba zdrowia. 86
3.3.11. Ubezpieczenia społeczne, majątkowe i osobowe. 86
3.3.12. Telekomunikacja. 88
3.3.13. Zatrudnienie. 89
3.3.14. Windykacja. 91
3.3.15. Inne. 93
3.4. Przekazywanie danych do państw trzecich. 93
4. Rozpatrywanie zawiadomień o naruszeniu danych osobowych. 99
5. Egzekwowanie obowiązków o charakterze niepieniężnym określonych w decyzjach administracyjnych GIODO. 100
6. Prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach. 106
7. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych. 116
8. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych 173
8.1. Interpretacja przepisów. 173
9. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. 279
9.4. Międzynarodowe konferencje, seminaria i spotkania. 285
9.5. Wizyty robocze. 293

Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2014 roku. 294

Część IV. Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych. 341

Załącznik nr 1 Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2014 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego 350

Załącznik nr 2 Wykaz kontroli przeprowadzonych w 2014 r. 354

Załącznik nr 3 Wykaz orzeczeń wydanych w 2014 r. przez Wojewódzki Sąd Administracyjny w Warszawie i Naczelny Sąd Administracyjny w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych 364
Załącznik nr 4 Informacje przekazane prz organy ścigania w sprawach zawiadomień o popełnieniu przestępstwa skier wany zez Generalnego ktora Ochrony Danych Osobowych w 2014 r. 81
Załącznik nr 5 Wykaz szkoleń przeprowadzonych przez GIODO w 2014 r. 382
Załącznik nr 6 Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych w 2014 r. 384
Załącznik nr 7 Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2014 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty 388
Załącznik nr 8 Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2014 r. za granicą 391

SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W 2014 ROKU

Wprowadzenie

W roku sprawozdawczym 2014 upłynęła IV kadencja i rozpoczęła się V kadencja Generalnego Inspektora Ochrony Danych, pełniona przez dra Wojciecha R. Wiewiórowskiego do czasu złożenia przez niego rezygnacji ze stanowiska Generalnego Inspektora Ochrony Danych Osobowych. W związku z wyborem na stanowisko zastępcy Europejskiego Inspektora Ochrony Danych, Wojciech Wiewiórowski w dniu 28 listopada 2014 r. złożył rezygnację z funkcji Generalnego Inspektora. Sejm 3 grudnia 2014 r. podjął uchwałę o odwołaniu go ze stanowiska GIODO, a Senat RP 18 grudnia 2014 r. wyraził na to zgodę. Od tego dnia, do czasu wyboru Generalnego Inspektora VI kadencji, dr Edyty Bielak-Jomaa, urzędem kierował Andrzej Lewiński, Zastępca GIODO.

Rok 2014 był również rokiem zmian we władzach Grupy Roboczej art. 29, niezależnego europejskiego organu doradczego Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności. W dniu 27 lutego 2014 r. na stanowisko Przewodniczącego Grupy Roboczej Art. 29 powołano Przewodniczącą francuskiego organu ochrony danych (CNIL) panią Isabelle Falque-Pierrotin. Wiceprzewodniczącymi zostali pan dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, oraz pan Gérard Lommel, Przewodniczący luksemburskiego organu ochrony danych.

W 2014 r. zakończyła się również kadencja Europejskiego Inspektora Ochrony Danych (EIOD)[2], którą od 2004 r. pełnił dwukrotnie Peter Hustinx.

Rok 2014 był również okresem intensywnych prac legislacyjnych, które doprowadziły do wprowadzenia istotnych zmian w ustawie o ochronie danych osobowych.

[2] (ang) European Data Protection Supervisor – EDPS.

Część I. Prawne podstawy działalności Generalnego Inspektora Ochrony Danych Osobowych.

1. Informacje ogólne.

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[3], która nałożyła na kraje członkowskie zobowiązanie stworzenia ustawodawstwa w zakresie ochrony danych osobowych.

Natomiast podstawowym dokumentem ustanawiającym unijne przepisy o ochronie danych osobowych jest **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.), 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.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182 z późn. zm.) stanowiła implementację ww. dyrektywy do polskiego porządku prawnego, przyczyniając się w ten sposób do stworzenia systemu ochrony danych osobowych w Polsce[4]. Ponadto Konstytucja RP – uchwalona w 1997 r. równolegle z ustawą o ochronie danych osobowych – w rozdziale „Wolności, prawa i obowiązki człowieka i obywatela" zagwarantowała obywatelom prawo do prywatności (art. 47), tajemnicy komunikacji (art. 49), zaś w art. 51 – prawo do ochrony informacji dotyczących własnej osoby. W ten sposób prawo do prywatności i ochrony danych osobowych, gwarantowane przez Konstytucję Rzeczypospolitej Polskiej, stało się jednym z fundamentów wolności obywatelskiej w demokratycznym państwie prawa.

Nad przestrzeganiem prawa obywateli do ochrony dotyczących ich danych osobowych czuwa Generalny Inspektor Ochrony Danych Osobowych - niezależny jednoosobowy organ

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

[4] 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.

administracji publicznej, który swym działaniem obejmuje zarówno sektor publiczny i prywatny.

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 2014 r. poz. 1182 z późn. zm.) oraz wydane na jej podstawie akty wykonawcze:

a) rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014, poz. 1934);

b) 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;

c) 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);

d) 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.

e) rozporządzenie 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.

W związku z ogłoszeniem ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r. poz. 1662), na mocy art. 9, który wszedł w życie - w dniu 1 stycznia 2015 r., nastąpiły zmiany przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zmiany dotyczyły funkcjonowania administratora bezpieczeństwa informacji oraz zwolnienia z obowiązku uzyskania zgody GIODO na przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, gdy ich przekazywanie odbywa się na podstawie standardowych klauzul umownych albo wiążących reguł korporacyjnych (nowe przepisy wprowadzają w polskim porządku prawnym instytucję wiążących reguł korporacyjnych oraz określają tryb ich zatwierdzenia przez GIODO).

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.

I tak, 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 nałożyła obowiązek zawiadamiania GIODO i abonentów o naruszeniu danych osobowych (art. 174a ust. 1) i prowadzenia rejestru takich zdarzeń (art. 174d ust. 1). 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).

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 2012 r. poz. 1015 z późn. zm.),
4. prowadzenia rejestru zbiorów danych oraz rejestru administratorów bezpieczeństwa informacji, a także udzielania informacji o zarejestrowanych zbiorach danych i zarejestrowanych administratorach bezpieczeństwa informacji,
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.

Postępowanie w sprawach uregulowanych w ustawie o ochronie danych osobowych, Generalny Inspektor prowadzi według przepisów Kodeksu postępowania administracyjnego (K.p.a.), o ile przepisy ustawy nie stanowią inaczej (art. 22).

2. Reforma ochrony danych osobowych w Unii Europejskiej.

W analizowanym 2014 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"**[5]. 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.

W dniu 25 stycznia 2012 r. Komisja Europejska przedstawiła w Brukseli projekt kompleksowej reformy unijnych przepisów o ochronie danych, który przewiduje zastąpienie dyrektywy 95/46/WE **rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych**[6] oraz 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**[7].

Parlament Europejski wskazał Komisję ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) jako odpowiedzialną za oba wnioski. 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

[5] Wniosek Komisji Europejskiej COM (2010) 609 wersja ostateczna.
[6] Wniosek Komisji Europejskiej COM (2012) 11 wersja ostateczna.
[7] Wniosek Komisji Europejskiej COM (2012) 10 wersja ostateczna.

Danych Osobowych aktywnie uczestniczył w posiedzeniach wspomnianych grup roboczych Rady UE.

W 2014 roku udało się zamknąć kolejny ważny etap negocjacji w pracach nad nowym prawem ochrony danych w UE. Parlament Europejski udzielił silnego poparcia dla reformy ochrony danych w UE, obejmującej zarówno ogólne rozporządzenie o ochronie danych, jak i dyrektywę o ochronie danych w kontekście egzekwowania prawa, głosując w dniu 12 marca 2014 r. za przyjęciem obydwu projektów[8]. Teraz kluczowe dla nowych przepisów będą prace w Radzie Unii Europejskiej.

W dniu 28 stycznia 2014 r. podczas obchodów VIII Dnia Ochrony Danych Osobowych podkreślano wagę prac nad europejską reformą ochrony danych osobowych i prywatności wskazując, że ma ona najwyższy priorytet spośród wielu zadań stojących przed rzecznikami ochrony danych osobowych. Bowiem za jej sprawą zasady ochrony prywatności i danych osobowych mogą stać się wzorcem do naśladowania dla reszty świata. Dzięki niej obywatele będą mieli kontrolę nad swoimi danymi dzięki unowocześnieniu sprawdzonych już zasad (np. prawo do usunięcia danych), ograniczeniu niepożądanych praktyk i wprowadzeniu większej przejrzystości tych, powszechnie stosowanych (np. w odniesieniu do profilowania), czy też poprzez wprowadzenie nowych zasad, takich jak prawo do przenoszenia danych oraz prawo do informacji o naruszeniu ochrony danych osobowych. W założeniu zasady te służyć mają ochronie prywatności obywateli, którzy chcą, aby usługi internetowe były godne zaufania. Ale skorzysta na tym również biznes, bo dla małych i średnich przedsiębiorców stworzony zostanie jednolity rynek z wieloma milionami konsumentów.

Nowe przepisy opierają się na czterech podstawowych filarach:

1. **jeden kontynent** – jedno prawo ze skutecznymi sankcjami;
2. **rozporządzenie ustanowi punkt kompleksowej usługi** – przedsiębiorstwa, które prowadzą działalność w kilku państwach UE oraz ich konsumenci będą mieli do czynienia z jednym krajowym organem nadzorczym;
3. **te same zasady dla wszystkich przedsiębiorstw, niezależnie od miejsca ich siedziby** – przedsiębiorstwa spoza Unii będą musiały przestrzegać europejskiego prawa ochrony danych, jeżeli prowadzą działalność na rynku europejskim;

[8] Więcej informacji na temat przebiegu głosowania w Parlamencie Europejskim znajduje się na stronach internetowych Parlamentu Europejskiego: http://www.europarl.europa.eu/news/pl/news-room/content/20140307IPR38204/html/Pos%C5%82owie-zaostrzaj%C4%85-zasady-ochrony-danych-osobowych-w-%C5%9Bwiecie-cyfrowym i Komisji Europejskiej: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm .

4. **prawo do bycia zapomnianym** (prawo żądania usunięcia danych) pozwala obywatelom na uzyskanie od stron trzecich (którym przekazano dane) usunięcia wszelkich linków do danych, kopii lub replikacji tych danych, zwłaszcza gdy brak jest uzasadnionego powodu do ich przechowywania.

Reforma ochrony danych jest ukierunkowana na pobudzenie wzrostu gospodarczego poprzez redukcję kosztów i biurokracji dla europejskich przedsiębiorstw, szczególnie dla małych i średnich przedsiębiorstw (MŚP). Po pierwsze, mając jedno prawo zamiast 28, reforma ochrony danych UE pomoże MŚP wejść na nowe rynki. Po drugie, Komisja Europejska zaproponowała zwolnienie MŚP z szeregu postanowień ogólnego rozporządzenia o ochronie danych, podczas gdy obecnie obowiązująca dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 1995 r. ma zastosowanie do wszystkich europejskich przedsiębiorstw, niezależnie od ich wielkości. Zgodnie z nowymi przepisami MŚP skorzystają z czterech ograniczeń biurokracji – zwolnienia z obowiązku powoływania urzędnika ds. ochrony danych (o ile przetwarzanie danych nie jest podstawową działalnością), brak konieczności dokonywania zgłoszeń, pobierania opłaty za zapewnienie dostępu w przypadku, gdy wnioski o dostęp do danych będą nadmierne w stosunku do celu lub gdy będą się powtarzały oraz – MŚP nie będą miały obowiązku przeprowadzenia oceny wpływu na ochronę prywatności (chyba, że będzie istniało określone zagrożenie).

Reforma nakłada na przedsiębiorstwa spoza Europy, ale które działają na europejskim rynku, obowiązek przestrzegania unijnych przepisów o ochronie danych. W przypadku ich naruszenia stosowane będą dotkliwe sankcje finansowe, które mogą wynieść nawet 2 % rocznych światowych obrotów przedsiębiorstwa. W odniesieniu do przepisów dotyczących przekazywania danych osobowych Europejczyków do państw trzecich, to władze takiego państwa – jeśli chcą mieć dostęp do danych obywateli UE – muszą zastosować ramy prawne uwzględniające kontrolę sądową. Bezpośrednie zwracanie się do firmy nie może stać się regułą. Dzięki temu obywatele europejscy będą mieli zapewnioną nie tylko ochronę, ale i gwarancję, że przekazywanie danych do państw trzecich nie oznacza rezygnacji z przysługujących im praw.

Reforma przyniesie wymierne korzyści także przedsiębiorcom, którzy prowadząc działalność w innych państwach członkowskich do tej pory musieli w każdym z nich spełniać określony zestaw zasad ochrony danych i komunikując się za każdym razem z innym organem ochrony danych osobowych. Wraz z reformą powstanie jedno prawo ochrony danych obowiązujące w całej Unii Europejskiej. Jeden kontynent – jedno prawo.

Udoskonalenie europejskich, wysokich standardów ochrony danych osobowych stanowi więc ogromną szansę dla rozwoju biznesu. Świadomość obywateli w zakresie prawa do prywatności i ochrony danych osobowych stale wzrasta, co jest konsekwencją cyfrowej rzeczywistości, do której przenoszą swoją aktywność. Przedsiębiorstwa zapewniające wyższy poziom bezpieczeństwa i ochrony danych osobowych znajdą się w czołówce. Gwarantowana przez nich wysoka dbałość o ochronę danych będzie ich atutem, decydującym o przewadze konkurencyjnej.

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. 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 2014 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.

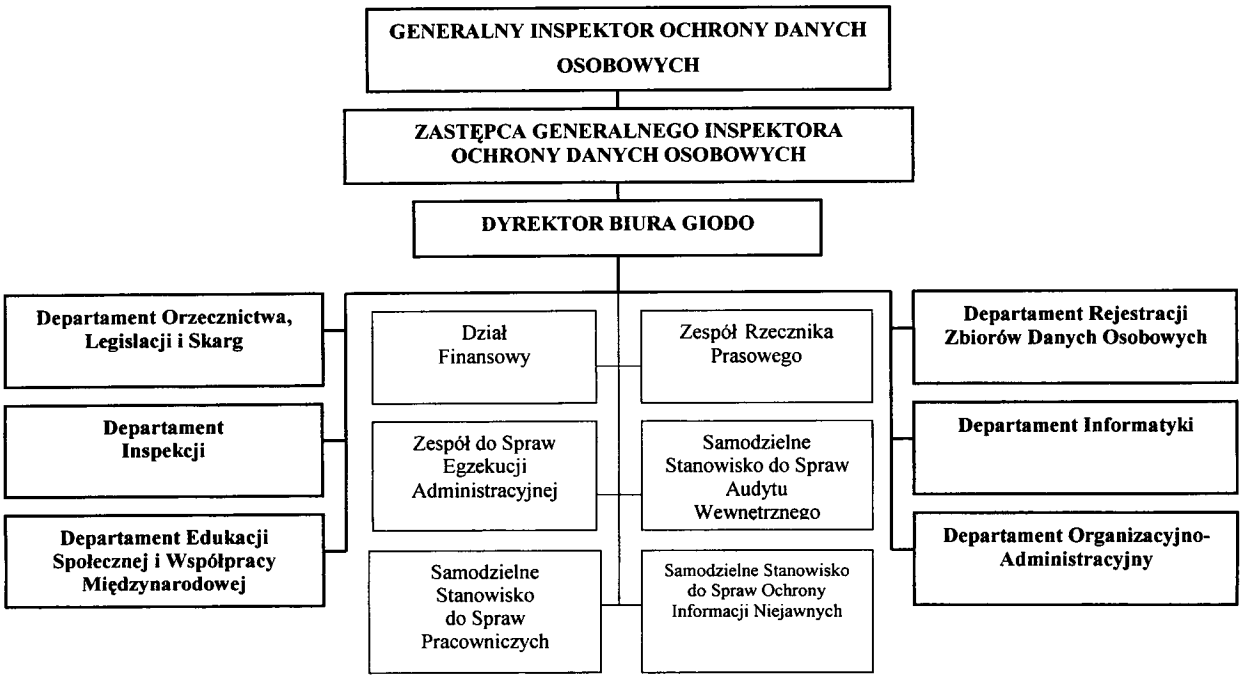
Prezydent Rzeczypospolitej Polskiej, po zasięgnięciu opinii Generalnego Inspektora, w drodze rozporządzenia nadaje statut Biuru, określając jego organizację, zasady działania, siedziby jednostek zamiejscowych oraz zakres ich właściwości terytorialnej, mając na uwadze stworzenie optymalnych warunków organizacyjnych 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. z 2011 r., 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:



Wykres 1. ***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[9].

[9] 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 2014 r. – 129,86 etatów (tj. 133 osoby), zaś na dzień 31 grudnia 2014 r. – **128,355** etatów (tj. 132 osoby). Na stanowiskach merytorycznych zatrudnionych było 116 osób, a na stanowiskach pomocniczych 16 osób. Wyższe wykształcenie posiadało 113 pracowników, w tym 77 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2014 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) – 4 osób (4 etaty)
- Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) – 11 osób (10,75 etatu),
- Departament Informatyki (DIF) – 15 osób (15 etatów),
- Departament Inspekcji (DIS) – 14 osób (14 etatów),
- Departament Organizacyjno-Administracyjny (DOA) – 18 osób (17,40 etatu),
- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 36 osób (36 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 (1,25 etatu),
- Samodzielne Stanowisko ds. Pracowniczych – 2 osoby (1,75 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 2014 r.

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2014 r. wynosił: **15 225** tys. zł. Plan po zmianach na 2014 r. przedstawiał się następująco:

- wynagrodzenia 9 351 tys. zł

- pochodnie od wynagrodzeń 1 661 tys. zł
- wydatki majątkowe 460 tys. zł
- pozostałe wydatki 3 753 tys. zł

Wydatki zrealizowane przez GIODO w 2014 roku w kwocie **15 018** tys. zł obejmowały:

- wynagrodzenia 9 298 tys. zł
- pochodne od wynagrodzeń 1 636 tys. zł
- wydatki majątkowe 437 tys. zł
- pozostałe wydatki 3 647 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[10]. 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.

[10] 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. Wymienionym uprawnieniom towarzyszy obowiązek kierownika jednostki kontrolowanej, umożliwienia inspektorom dokonania tych czynności (art. 15 ust. 1 ustawy o ochronie danych osobowych).

Przeprowadzane w toku kontroli czynności (odbieranie wyjaśnień od kierownictwa i pracowników kontrolowanej jednostki, oględziny) są dokumentowane w formie protokołów przyjęcia ustnych wyjaśnień, protokołów przesłuchania w charakterze świadka oraz protokołów oględzin miejsca, pomieszczeń, dokumentów, urządzeń, nośników, systemów informatycznych służących do przetwarzania danych osobowych. Na podstawie ustaleń zawartych w ww. protokołach, analizy dokumentów przedłożonych w toku kontroli (stanowiących w szczególności uchwały i zarządzenia organów reprezentujących jednostkę kontrolowaną, regulaminy, instrukcje i procedury określające zasady przetwarzania danych osobowych, zawarte umowy, w tym umowy powierzenia przetwarzania danych osobowych oraz opracowane formularze i kwestionariusze) oraz wydruków z systemów informatycznych

służących do przetwarzania danych osobowych, sporządzany jest protokół kontroli. Podpisany przez inspektorów, którzy kontrolę przeprowadzili, protokół ten przedstawiany jest następnie do podpisu kierownikowi jednostki kontrolowanej, który zgodnie z art. 16 ust. 2 ustawy o ochronie danych osobowych może wnieść do niego umotywowane zastrzeżenia i uwagi. W zależności od ustaleń poczynionych w toku kontroli, tzn. czy stwierdzone zostały nieprawidłowości w procesie przetwarzania danych osobowych, wszczynane jest postępowanie administracyjne lub kierowane jest do jednostki kontrolowanej pismo z informacją, że w zakresie objętym kontrolą nie stwierdzono uchybień. 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 2014 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **175 kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych.

2.2.1. Administracja publiczna.

W 2014 r. w podmiotach wykonujących zadania publiczne przeprowadzono **25 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W ramach tej kategorii podmiotów kontrole przeprowadzono m.in. w 11 podmiotach w związku z wymianą informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy (korzystających ze świadczeń pomocy społecznej lub ubiegających się o takie świadczenie) pomiędzy jednostkami organizacyjnymi pomocy społecznej i jednostkami obsługującymi świadczenia rodzinne a powiatowymi urzędami pracy[11].

Jak ustalono w toku przeprowadzonych kontroli, podstawę prawną dla wymiany informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy (korzystających ze świadczeń pomocy społecznej lub ubiegających się o takie świadczenie) pomiędzy jednostkami organizacyjnymi pomocy społecznej i jednostkami obsługującymi

[11] Np. kontrole DIS-K-421/59/14, DIS-K-421/77/14 i DIS-K-421/94/14.

świadczenia rodzinne a powiatowymi urzędami pracy, stanowi art. 33 ust. 7 i 7a ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz. U. z 2013 r. poz. 674 z późn. zm.)[12]. Wskazane przepisy w swoim obecnym kształcie obowiązują od dnia 27 maja 2014 r., tj. od wejścia w życie znowelizowanych przepisów ustawy o promocji zatrudnienia i instytucjach rynku pracy, na mocy ustawy z dnia 14 marca 2014 r. o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw (Dz. U. z 2014 r. poz. 598). Przed dniem 27 maja 2014 r. przepisy ww. ustawy dopuszczały wyłącznie udostępnianie przez powiatowe urzędy pracy informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy jednostkom organizacyjnym pomocy społecznej oraz jednostkom obsługującym świadczenia rodzinne. Przesądzała o tym treść obowiązującego wówczas art. 33 ust. 7 powołanej ustawy[13]. Dopiero dodanie ustępu 7a w art. 33 dało podstawę powiatowym urzędom pracy do pozyskiwania ww. informacji z jednostek organizacyjnych pomocy społecznej oraz z jednostek obsługujących świadczenia rodzinne.

Kontrole wykazały, że wymiana drogą elektroniczną informacji o ww. osobach pomiędzy jednostkami organizacyjnymi pomocy społecznej i jednostkami obsługującymi świadczenia rodzinne a powiatowymi urzędami pracy, następowała w 5 poddanych kontroli podmiotach i odbywała się w obrębie jednostek działających na tym samym obszarze (np. gmina, powiat), przy czym w 3 przypadkach była ona jednokierunkowa, tzn. dane były udostępniane wyłącznie przez powiatowe urzędy pracy jednostkom organizacyjnym pomocy społecznej. W pozostałych skontrolowanych jednostkach taka wymiana nie była prowadzona lub miała miejsce na podstawie wniosków składanych w sposób tradycyjny (tj. w formie papierowej).

[12] Art. 33 ust. 7. Informacje, o których mowa w ust. 6, są udostępniane publicznym służbom zatrudnienia lub innym podmiotom, realizującym 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 szczególności jednostkom organizacyjnym pomocy społecznej oraz jednostkom obsługującym świadczenia rodzinne. Art. 33 ust. 7a. Informacje, o których mowa w ust. 6, w zakresie niezbędnym do realizacji zadań określonych w ustawie, mogą być pozyskiwane przez powiatowe urzędy pracy z publicznych służb zatrudnienia lub innych podmiotów, w szczególności jednostek organizacyjnych pomocy społecznej oraz jednostek obsługujących świadczenia rodzinne, realizujących zadania na podstawie ustawy lub odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny.

[13] Art. 33 ust. 7 (w brzmieniu sprzed dnia 27 maja 2014 r.). Informacje, o których mowa w ust. 6, mogą być udostępniane w trybie i na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne na podstawie wniosku złożonego w szczególności w formie dokumentu elektronicznego innym podmiotom, w szczególności jednostkom organizacyjnym pomocy społecznej oraz jednostkom obsługującym świadczenia rodzinne, realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny w zakresie niezbędnym do realizacji tych zadań. Dostęp do danych osobowych jest nadzorowany i rejestrowany zgodnie z przepisami o ochronie danych osobowych.

Do wymiany informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy, które korzystają ze świadczeń pomocy społecznej lub ubiegają się o takie świadczenie, podmioty uczestniczące w tej wymianie wykorzystywały dedykowany system informatyczny, opracowany przez podmiot prywatny. Jak ustalono, istniały dwa modele wdrażania ww. systemu: model lokalny (w oparciu o serwer zainstalowany w powiatowym urzędzie pracy) oraz model centralny (w oparciu o serwer centralny, znajdujący się w podmiocie, który opracował ten system).

Zasady wymiany informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy, które korzystają ze świadczeń pomocy społecznej lub ubiegają się o takie świadczenie, pomiędzy konkretnymi jednostkami organizacyjnymi pomocy społecznej lub jednostkami obsługującymi świadczenia rodzinne a powiatowymi urzędami pracy, a w szczególności zakres danych, które takiej wymianie mogą podlegać, określono w porozumieniach lub umowach w sprawie zasad i zakresu udostępniania danych. Zakres ten obejmuje m.in. dane osobowe beneficjenta (imię, nazwisko, PESEL, datę urodzenia, rodzaj i nr dokumentu tożsamości, płeć, stan cywilny, adres zamieszkania), okres rejestracji w powiatowym urzędzie pracy, przyznane świadczenia i zasiłki, proponowane i odbyte szkolenia, wykształcenie i kwalifikacje zawodowe oraz historię zatrudnienia.

Na podstawie dokonanych ustaleń stwierdzono, że wymiana danych odbywała się w sposób zgodny z wymogami wynikającymi z przepisów o ochronie danych oraz przepisów ustawy o promocji zatrudnienia i instytucjach rynku pracy, a w szczególności z wymogami określonymi w art. 33 ust. 8 ustawy o promocji zatrudnienia i instytucjach rynku pracy, w którym m.in. określone zostały wymogi, jakie musi spełniać system informatyczny wykorzystywany do takiej wymiany danych[14]. Stwierdzone w toku kontroli uchybienia dotyczyły dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i polegały na nieujęciu systemu informatycznego wykorzystywanego do wymiany danych w wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, niezawarciu w polityce bezpieczeństwa opisu struktury zbiorów

[14] Art. 33 ust. 8. Informacje, o których mowa w ust. 6, mogą być pozyskiwane, wymieniane lub udostępniane na wniosek złożony, w szczególności w postaci elektronicznej, w trybie i na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne lub zwykorzystaniem systemów teleinformatycznych, jeżeli powiatowy urząd pracy oraz podmiot, o którym mowa w ust. 7, spełniają łącznie następujące warunki: 1) posiadają możliwość identyfikacji osoby uzyskującej informacje w systemie oraz zakresu, daty i celu ich uzyskania; 2) posiadają zabezpieczenia uniemożliwiające wykorzystanie informacji niezgodnie z celem ich uzyskania; 3) zapewniają, że dostęp do danych osobowych jest nadzorowany i rejestrowany zgodnie z przepisami o ochronie danych osobowych.

danych, wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposobu przepływu danych pomiędzy poszczególnymi systemami, uwzględniających ww. system oraz niezawarciu w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych informacji na temat wdrożonego oprogramowania antywirusowego.

Wobec podmiotów, w których stwierdzono uchybienia dające podstawę do zastosowania środków, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych[15], wszczęte zostały postępowania administracyjne i wydane zostały decyzje nakazujące usunięcie uchybień lub decyzje umarzające postępowanie w odniesieniu do nieprawidłowości usuniętych w toku prowadzonych postępowań.

Kontrole w związku z wymianą informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy nie były jednak jedynymi kontrolami, które zostały przeprowadzone w okresie sprawozdawczym w podmiotach wykonujących zadania publiczne. Przykładem może być kontrola dotycząca przetwarzania przez prezydenta jednego z miast, danych osobowych mieszkańców biorących udział w konsultacjach społecznych w sprawie budżetu obywatelskiego.[16] Konsultacje społeczne były przeprowadzone na zasadach określonych w uchwale rady miasta, w sprawach zasadniczych dla rozwoju miasta, w tym m.in. projektu jego budżetu. W toku kontroli ustalono, że do tej pory przeprowadzone zostały dwie edycje konsultacji społecznych z mieszkańcami. Wszystkie osoby biorące udział w głosowaniu nad ww. budżetem obywatelskim były zobowiązane do wypełnienia formularza do głosowania, natomiast osoby zgłaszające projekty do realizacji w ramach tego budżetu do wypełnienia formularza zgłaszania projektów.

W związku z pierwszą edycją budżetu obywatelskiego, weryfikacja danych osobowych dotyczyła jedynie ustalenia, czy na każdej karcie do głosowania wpisane zostało imię i nazwisko osoby głosującej oraz numer PESEL tej osoby. Przy tej edycji nie dokonywano weryfikacji tożsamości osoby głosującej na podstawie informacji zawartych w ewidencji ludności prowadzonej przez urząd miasta. Natomiast w trakcie drugiej edycji taka weryfikacja została przeprowadzona.

---

[15] 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.

[16] Kontrola DIS-K-421/42/14

W związku z udziałem mieszkańców w głosowaniu nad budżetem obywatelskim dane tych osób przetwarzane były na podstawie przepisów prawa w oparciu o podstawę wskazaną - w art. 23 ust 1 pkt 2 ustawy o ochronie danych osobowych. Jak wynika bowiem z art. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 1990 r. Nr 16 poz. 95), mieszkańcy gminy (miasta na prawach powiatu) z mocy prawa tworzą wspólnotę samorządową, a więc są podstawowym, obywatelskim składnikiem jednostki samorządu terytorialnego i posiadają prawo (na zasadach przewidzianych w ustawach) do udziału w życiu publicznym wspólnoty samorządowej. Zgodnie zaś z art. 5a ustawy o samorządzie gminnym w wypadkach przewidzianych ustawą oraz w innych sprawach ważnych dla gminy mogą być przeprowadzone na jej terytorium konsultacje z mieszkańcami gminy. Dane projektodawców (tj. osób zgłaszających projekty do realizacji w ramach budżetu obywatelskiego) przetwarzanie były na podstawie przesłanki wskazanej w art. 23 ust 1 pkt 1 ustawy o ochronie danych osobowych[17], tj. na podstawie zgody wyrażonej przez osoby, których dane dotyczą. Osobom zgłaszającym projekty w II edycji nie były natomiast przekazywane informacje, o których mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych[18].

W toku kontroli ustalono, że prowadzone postępowania w sprawach konsultacji społecznych w sprawie budżetu obywatelskiego zostały zakończone, a wszystkie dane osobowe pozyskane za pomocą formularzy do głosowania (w wersji papierowej i elektronicznej) usunięto.

Wobec powyższego, Generalny Inspektor nie skorzystał z prawa określonego w art. 18 ust. 1 pkt 1 ustawy o ochronie danych osobowych[19]. Niemniej jednak Generalny Inspektor poinformował prezydenta miasta, iż zgodnie z art. 24 ust. 1 pkt 4 ustawy o ochronie danych osobowych, w przypadku zbierania danych osobowych od osoby, której one dotyczą,

---

[17] Art. 23. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych.

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

[19] Art. 18 ust. 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.

administrator danych jest obowiązany poinformować tę osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje o jego podstawie prawnej. Wskazał ponadto, iż zasadne byłoby, żeby osoby wypełniające w przyszłości formularze, o których mowa powyżej, posiadały informację, iż dane ich pozyskiwane są na podstawie uchwały w sprawie zasad i trybu przeprowadzenia konsultacji społecznych na terenie miasta.

W toku innej kontroli, której poddano jeden z urzędów miasta[20], stwierdzono, że burmistrz miasta przetwarza dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych, stanowiące wizerunki osób przebywających w obszarze objętym monitoringiem budynku tego urzędu, zarejestrowanych poprzez kamery monitoringu i utrwalone w celu zapewnienia bezpieczeństwa osób i mienia w budynku. W związku z tym, że zestaw ww. danych osobowych jest dostępny według określonych kryteriów, to jest czasu i miejsca nagrania, stanowi on zbiór danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych[21]. Zbiór ten powinien zostać zgłoszony do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, ponieważ nie mają tu zastosowania przesłanki określone w art. 43 ust. 1 ustawy o ochronie danych osobowych, zwalniające z obowiązku rejestracji[22]. Burmistrz nie dokonał zgłoszenia ww. zbioru.

---

[20] Kontrola DIS-K-421/13/14

[21] Art. 7 pkt 1. Przez zbiór danych rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

[22] Art. 43. 1. 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 Wizowym Systemie Informacyjnym; 2c) przetwarzanych przez właściwie 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; 12) przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1. 1a. Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1, nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go Generalnemu Inspektorowi do rejestracji, z zastrzeżeniem art. 46e ust. 2.

W związku ze stwierdzonym uchybieniem w procesie przetwarzania danych osobowych, o którym mowa powyżej, zostało wszczęte postępowanie administracyjne. W toku prowadzonego postępowania usunięto ww. uchybienie i z tego względu postępowanie zostało umorzone na mocy decyzji administracyjnej[23] wydanej przez Generalnego Inspektora Ochrony Danych Osobowych.

Do interesujących kontroli należała również kontrola przeprowadzona w spółce realizującej projekty współfinansowane ze środków Europejskiego Funduszu Społecznego - podstawie umów zawieranych z urzędami administracji publicznej[24]. W związku z realizacją ww. projektów, spółka przetwarzała dane osobowe kandydatów na uczestników projektów, dane osobowe uczestników tych projektów oraz dane osobowe przedsiębiorców kierujących osoby do uczestnictwa w projektach. Jak ustalono, przetwarzanie tych danych zostało powierzone wybranej spółce, stosownie do art. 31 ustawy o ochronie danych osobowych[25], przez Ministra Infrastruktury i Rozwoju. Wobec osób, które zgłosiły się do uczestnictwa w projekcie, ale ostatecznie nie wzięły w nim udziału (nie zostały zakwalifikowane lub zostały zakwalifikowane, ale zrezygnowały z uczestnictwa w projekcie) oraz przedsiębiorców zgłaszających pracowników do udziału w projektach, administrator danych nie realizował obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych osobowych.

Ustalono ponadto, że niektóre z projektów były kierowane m.in. do osób niepełnosprawnych. W treści formularza zgłoszeniowego kandydat na uczestnika projektu składał oświadczenie, że jest osobą niepełnosprawną. Na podstawie zebranego materiału dowodowego uznano, iż administrator danych, tj. Minister Infrastruktury i Rozwoju, nie legitymuje się którąkolwiek z przesłanek, o których mowa w art. 27 ust. 2 ustawy o ochronie danych osobowych [26], przetwarzania danych ujawniających stan zdrowia (jakimi są

[23] Decyzja DIS/DEC-446/14/35683
[24] Kontrola DIS-K-421/103/14
[25] Art. 31 ust. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
[26] 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 pkt 1 i pkt 2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli: osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych; przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony.

informacje o niepełnosprawności) kandydatów do udziału w projekcie oraz tych osób, które zostały zakwalifikowane i nie zrezygnowały z udziału w projekcie (uczestników projektu).

W wyniku kontroli przeprowadzonej w jednym ze starostw powiatowych[27] stwierdzono, że na stronie internetowej tego podmiotu, służącej m.in. do przeglądania map geodezyjnych, do dnia 31 sierpnia 2014 r. były upubliczniane dane osobowe właścicieli nieruchomości w zakresie numerów ksiąg wieczystych tych nieruchomości. Ustalenia wykazały, że w kontrolowanym starostwie w dniu 1 września 2014 r. zainstalowany został nowy system informatyczny służący do kompleksowego prowadzenia zasobu geodezyjnego i kartograficznego, posiadający moduł służący do prowadzenia zasobu geodezyjnego i kartograficznego oraz moduł służący do udostępniania i publikacji danych dotyczących zasobu geodezyjnego i kartograficznego na stronie internetowej ww. starostwa powiatowego.

Dokonana zmiana systemu informatycznego służącego do udostępniania i publikacji danych dotyczących zasobu geodezyjnego i kartograficznego spowodowała, iż w kontrolowanym starostwie brak jest już dostępu za pomocą strony internetowej służącej m.in. do przeglądania map geodezyjnych, do danych osobowych właścicieli nieruchomości w zakresie numeru księgi wieczystej właściciela nieruchomości i dane te nie są upubliczniane.

2.2.2. Bezpieczeństwo publiczne.

W 2014 r. Generalny Inspektor przeprowadził **20 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, Biurze Ochrony Rządu, jednostkach Żandarmerii Wojskowej, sądach, prokuraturach oraz w konsulatach przy ambasadach Rzeczypospolitej Polskiej[28].** 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. z 2014 r. poz. 1203 z późn. zm.), tj. wglądu oraz dokonywania wpisów do SIS i VIS.

---

[27] Sygn. DIS-K-421/151/14

[28] Np. kontrole DIS-K-421/24/14, DIS-K-411/33/14, DIS-K-411/95/14, DIS-K-411/121/14, DIS-K-421/140/14.

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[29]) na wniosek Komendanta Głównego Policji w związku z dokonywanymi zmianami w KSI, polegającymi na zakończeniu prac technicznych związanych z realizacją projektu migracji Krajowego Systemu Informatycznego w zakresie Systemu Informacyjnego Schengen drugiej generacji na nową platformę sprzętową. Wskazany wniosek został złożony w trybie art. 34 ust. 1 ww. ustawy[30]. W wyniku ustaleń kontroli przeprowadzonej w Komendzie Głównej Policji, Generalny Inspektor wydał pozytywną opinię w zakresie zmian wprowadzonych w KSI uznając, iż spełnione zostały wymogi określone w art. 36-39 ustawy 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 o ochronie danych osobowych. Jedynie w toku kontroli przeprowadzonej w jednym z organów[31] uprawnionych do dostępu do Krajowego Systemu Informatycznego (KSI) w celu dokonywania wpisów oraz wglądu do danych SIS ustalono, że sprawdzenia danych w SIS dokonywane były także w ramach prowadzonych postępowań sprawdzających, w związku z przyznawaniem dostępu do informacji niejawnych oraz postępowaniem kwalifikacyjnym na wolne stanowiska pracy. Mając powyższe na uwadze GIODO uznał, że uprawnienie ww. organu do bezpośredniego dostępu do KSI w celu wglądu do danych SIS dotyczące osób, które biorą udział w postępowaniu kwalifikacyjnym na wolne stanowiska pracy oraz osób w związku z prowadzonym postępowaniem sprawdzającym do dostępu do informacji niejawnych w celu wydania poświadczenia bezpieczeństwa, było realizowane niezgodnie z przepisami ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, bowiem dokonywanie

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

[30] 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.

[31] Kontrola DIS-K-421/24/14

sprawdzeń danych osób w ww. celach nie znajdowało podstaw prawnych w tych przepisach. Kontrolowany organ argumentował, że dokonywanie sprawdzeń ww. osób w Systemie Informacyjnym Schengen w celu wglądu do danych SIS było realizowane na podstawie art. 25 ust. 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228)[32]. Analizując zaprezentowaną argumentację GIODO stwierdził, iż ww. przepis nie może stanowić podstawy do dokonywania sprawdzeń danych w Systemie Informacyjnym Schengen wobec osób, które biorą udział w postępowaniu kwalifikacyjnym do pracy w kontrolowanym organie oraz osób poddanych sprawdzeniu w ramach postępowania sprawdzającego w sprawie dostępu do informacji niejawnych w celu wydania poświadczenia bezpieczeństwa, z uwagi na to, iż powołany przepis wskazuje, iż osoby te powinny być sprawdzone w ewidencjach i kartotekach niedostępnych powszechnie. Systemu Informacyjnego Schengen nie można uznać za ewidencję lub kartotekę w rozumieniu tych przepisów. Jednocześnie, jak już wyżej wskazano, przepisy ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym nie wskazują, iż dla takich celów ww. sprawdzenie może być zrealizowane.

Z uwagi na stwierdzone uchybienia w procesie przetwarzania danych osobowych, wobec poddanego kontroli organu zostało wszczęte postępowanie administracyjne. W toku postępowania organ usunął uchybienia stanowiące przedmiot postępowania, co skutkowało jego umorzeniem[33].

2.2.3. Banki i inne instytucje finansowe.

W okresie sprawozdawczym w podmiotach należących do sektora banków i innych instytucji finansowych zostało przeprowadzonych **6 kontroli.**

Do jednej z bardziej interesujących kontroli należała kontrola przeprowadzona w banku w związku ze zgłoszeniem przez ten bank do rejestracji Generalnemu Inspektorowi zbioru danych dotyczących karalności agentów i ich pracowników oraz partnerów sprzedaży[34]. Kontrola wykazała, że bank podejmował współpracę w zakresie pośrednictwa finansowego z przedsiębiorcami na podstawie umów agencyjnych. W zależności od zakresu ww. współpracy podmioty te pełniły rolę agentów lub partnerów sprzedaży. Jednym z wymogów, który musiał

[32] Art. 25 ust. 1 pkt 2 ustawy o ochronie informacji niejawnych. Zwykłe postępowanie sprawdzające obejmuje: sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

[33] Decyzja DIS/DEC-765/14/59716

[34] Kontrola DIS-K-421/51/14

spełnić podmiot (przedsiębiorca) zamierzający współpracować z bankiem w zakresie pośrednictwa finansowego, było przekazanie danych osób reprezentujących dany podmiot - oraz danych pracowników (w przypadku agentów), którzy mieli wykonywać czynności powierzone przez bank. Podmioty te były zobowiązane do przekazania m.in. dotyczących tych osób zaświadczeń o niekaralności z Krajowego Rejestru Karnego. Ponadto w toku realizacji zawartych umów agencyjnych bank pozyskiwał od osób reprezentujących agentów i partnerów sprzedaży oświadczenia dotyczące ich niekaralności.

Generalny Inspektor uznał jednak, że przetwarzanie danych o niekaralności przedsiębiorców (osób reprezentujących agentów, partnerów sprzedaży) oraz pracowników agentów odbywało się bez podstawy prawnej, o której mowa w art. 27 ust. 2 ustawy o ochronie danych osobowych. Organ nie przychylił się do stanowiska banku wskazującego, że uzasadnieniem dla żądania przez bank danych o niekaralności od przedsiębiorców (osób reprezentujących agentów, partnerów sprzedaży) oraz pracowników agentów realizujących usługi finansowe na rzecz banku, była konieczność zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Bank wskazał jako podstawę prawną przetwarzania ww. danych § 3 uchwały Komisji Nadzoru Finansowego z dnia 20 grudnia 2012 r. Nr 359/2012 w sprawie wykazu dokumentów dotyczących działalności gospodarczej przedsiębiorcy lub przedsiębiorcy zagranicznego załączanych do wniosku o udzielanie zezwoleń, o których mowa w art. 6a ust. 1 pkt 1 lit m oraz art. 6d ust. 1 ustawy Prawo bankowe (Dz. Urz. KNF 2013, poz. 4)[35] oraz art. 758[36] i art. 760[37] Kodeksu cywilnego, a

[35] W przypadku przedsiębiorcy lub przedsiębiorcy zagranicznego, o którym mowa w § 1 ust. 1 pkt 1 lub 2, będącego osobą fizyczną, bank do wniosku o udzielenie zezwolenia, o którym mowa w § 1 ust. 1 pkt 1 lub 2, oprócz dokumentów, w tym oświadczeń, wymienionych w § 2, załącza: 1) pisemne oświadczenie przedsiębiorcy lub przedsiębiorcy zagranicznego o toczących się lub prowadzonych wobec niego w okresie trzech lat przed złożeniem wniosku o udzielenie zezwolenia postępowaniach karnych, karnych skarbowych, dyscyplinarnych lub egzekucyjnych, mogących mieć negatywny wpływ na jego sytuację finansową; 2) zaświadczenie o niekaralności wydane nie wcześniej niż na 3 miesiące przed datą złożenia wniosku o wydanie zezwolenia przez właściwy organ państwa, którego obywatelstwo posiada przedsiębiorca lub przedsiębiorca zagraniczny oraz przez właściwy organ państwa, w którym prowadzi on działalność gospodarczą, jeżeli jest to państwo inne niż państwo, którego obywatelstwo posiada przedsiębiorca, o ile w państwach tych wydawane są takie zaświadczenia; 3) poświadczoną notarialnie lub w sposób równorzędny w rozumieniu prawa miejsca zamieszkania lub siedziby przedsiębiorcy lub przedsiębiorcy zagranicznego kopię rocznego zeznania lub deklaracji podatkowej za rok podatkowy poprzedzający złożenie wniosku o udzielenie zezwolenia, sporządzone według przepisów obowiązujących w państwie, w którym podlega on obowiązkowi podatkowemu, bądź oświadczenie o braku możliwości przedłożenia wymaganych dokumentów wraz ze stosownym uzasadnieniem.

[36] Art. 758. Przez umowę agencyjną przyjmujący zlecenie (agent) zobowiązuje się, w zakresie działalności swego przedsiębiorstwa, do stałego pośredniczenia, za wynagrodzeniem, przy zawieraniu z klientami umów na rzecz dającego zlecenie przedsiębiorcy albo do zawierania ich w jego imieniu. Do zawierania umów w imieniu dającego zlecenie oraz do odbierania dla niego oświadczeń agent jest uprawniony tylko wtedy, gdy ma do tego umocowanie.

[37] Art. 760. Każda ze stron obowiązana jest do zachowania lojalności wobec drugiej.

także zaznaczył, że był zobowiązany na podstawie art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2012 r. poz. 1376 z późn. zm.) do dokładania szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych.

Treść art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych przesądza o tym, że tylko przepis zawarty w akcie normatywnym o randze ustawy może zezwolić na przetwarzanie „wrażliwych" danych osobowych. Jednocześnie brzmienie przepisu ustawy szczególnej nie powinno pozostawiać wątpliwości, iż zezwala on na przetwarzanie takich danych, w tym przypadku danych dotyczących niekaralności. Zatem, powoływanie się przez bank na postanowienia uchwały Komisji Nadzoru Finansowego nie mogło stanowić podstawy prawnej do pozyskiwania danych o niekaralności ww. osób. Również z powołanych przez bank przepisów Kodeksu cywilnego nie wynika, iż bank mógł kwestionowane dane pozyskiwać. Ponadto warunki, na jakich bank może powierzyć innemu przedsiębiorcy wykonanie czynności faktycznych związanych z działalnością bankową, zostały określone w art. 6a-6c ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r., poz. 1376 z późn. zm.). Generalny Inspektor uznał, że żaden z tych przepisów nie wskazuje, iż podmioty i pracownicy tych podmiotów są zobowiązani do składania dokumentów potwierdzających ich niekaralność.

W toku kontroli ustalono także, że z partnerami sprzedaży, którzy współpracowali z bankiem w zakresie promocji produktów oferowanych przez bank, podpisywane były umowy o współpracy polegającej na promowaniu produktów banku wśród klientów. Partnerzy ci nie byli upoważnieni do dokonywania jakichkolwiek czynności prawnych na rzecz banku. W celu podjęcia przez partnera sprzedaży współpracy z bankiem we ww. zakresie, był on zobowiązany do złożenia dokumentów dotyczących prowadzonej działalności gospodarczej oraz do przedstawienia innych dokumentów, tj. m.in. zaświadczenia o niekaralności wydanego przez Krajowy Rejestr Karny (zaświadczenie to dotyczyło osób reprezentujących dany podmiot). W ten sposób bank jednocześnie pozyskiwał pisemną zgodę na przetwarzanie danych ww. osób dotyczącą ich niekaralności. Ponadto w toku realizacji zawartych umów o współpracy bank pozyskiwał również od osób reprezentujących partnerów sprzedaży oświadczenia dotyczące ich niekaralności. Generalny Inspektor uznał, że pozyskiwanie danych o niekaralności osób reprezentujących partnerów sprzedaży, którzy współpracują z bankiem we ww. zakresie, było nieadekwatne w stosunku do celów, w jakich były przetwarzane, tj. promocji produktów oferowanych przez bank.

W toku kontroli ustalono także, iż osoby reprezentujące kandydatów na agentów oraz pracownicy agentów byli zobowiązani do przedstawienia m.in. pochodzących z Biura Informacji Kredytowej informacji o zobowiązaniach kredytowych. Pracownik (osoba zatrudniona przez agenta na podstawie umowy o pracę) przekazywał do banku ww. dokumenty za pośrednictwem agenta (tj. pracodawcy). Dane te były przetwarzane przez bank w związku z zawarciem i realizacją umowy agencyjnej. Zdaniem banku informacje i dane zawarte w raporcie przygotowanym przez Biuro Informacji Kredytowej, tj. dane o zobowiązaniach finansowych reprezentantów agentów i jego pracowników, były przetwarzane w celu oceny kompetencji i wiarygodności finansowej tych osób w związku z zawarciem i realizacją umowy agencyjnej, a także w celu zapewnienia bezpieczeństwa środków pieniężnych.

Generalny Inspektor uznał, iż pozyskiwanie danych zawartych w raportach przygotowanych przez Biuro Informacji Kredytowej dotyczących ww. osób było nieadekwatne w stosunku do celów, w jakich były one przetwarzane. Wskazał, że przedmiotowe dane winny być wykorzystywane przez uprawnione podmioty zgodnie z przepisami Prawa bankowego, tj. przede wszystkim w celu dokonania przez te podmioty oceny zdolności kredytowej i analizy ryzyka kredytowego, a nie w celu zawierania i realizacji umów agencyjnych. Zbieranie przez agentów zaświadczeń o niekaralności od pracowników współpracujących z bankiem w zakresie pośrednictwa finansowego, prowadziło do naruszenia przez te podmioty przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. Nr 21, poz. 94 z późn. zm.), które w art. 22^1 określiły dopuszczalny zakres danych osobowych, jakie pracodawca może zbierać od pracowników. Jednocześnie żaden przepis prawa, a w szczególności Prawa bankowego, nie pozwala na rozszerzenie określonego w art. 22^1 Kodeksu pracy katalogu danych, które mogą być pozyskiwane od pracowników. Powyższa sytuacja dotyczy także zbierania od pracowników agentów, danych o zobowiązaniach finansowych pochodzących z Biura Informacji Kredytowej.

Z uwagi na stwierdzone uchybienia w procesie przetwarzania danych osobowych, wobec banku zostało wszczęte postępowanie administracyjne. W toku postępowania bank usunął uchybienia stanowiące przedmiot postępowania poprzez zaprzestanie przetwarzania oraz usunięcie danych dotyczących karalności oraz danych o zobowiązaniach finansowych, w

szczególności pochodzących z Biura Informacji Kredytowej. Z powyższych względów postępowanie w tym zakresie zostało umorzone[38].

Ponadto w przedmiotowej sprawie Generalny Inspektor wystąpił do Przewodniczącego Komisji Nadzoru Finansowego o podjęcie niezbędnych działań mających na celu zmianę treści uchwały Komisji Nadzoru Finansowego z dnia 20 grudnia 2012 r. Nr 359/2012 r. w sprawie wykazu dokumentów dotyczących działalności gospodarczej przedsiębiorcy lub przedsiębiorcy zagranicznego, załączanych do wniosku o udzielanie zezwoleń, o których mowa w art. 6a ust. 1 pkt 1 lit m oraz art. 6d ust. 1 ustawy - Prawo bankowe (Dz. Urz. KNF 2013, poz. 4), w zakresie zapewnienia zgodności ww. uchwały z przepisami o ochronie danych osobowych. W odpowiedzi na ww. wystąpienie Przewodniczący Komisji Nadzoru Finansowego poinformował, iż w Ministerstwie Finansów prowadzone są prace nad projektem ustawy o zmianie ustawy Prawo bankowe.

W toku kontroli[39] przeprowadzonej w spółce, której działalność polega na udzielaniu pożyczek w oparciu o przepisy ustawy z dnia 24 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2014 r. poz. 121 z późn. zm.) oraz ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim (Dz. U. Nr 126, poz. 715 z późn. zm.), stwierdzono, że przetwarzała ona dane osobowe klientów w celu zawarcia oraz realizacji umowy pożyczki, marketingu swoich produktów i usług, jak również w celach windykacyjnych. Badając podstawy prawne przetwarzania danych osobowych klientów stwierdzono, że spółka pozyskiwała zgodę na przetwarzanie tych danych w celach, których nie realizowała lub w ogóle takich celów nie określiła. Ponadto w jednym oświadczaniu o wyrażeniu zgody na przetwarzanie danych osobowych łączyła różne cele ich przetwarzania. Ustalono również że spółka przetwarzała w celach marketingowych dane osób, z którymi nie została zawarta umowa pożyczki; jednocześnie spółka nie dysponowała inną podstawą prawną do przetwarzania tych danych, bowiem ustał cel (zawarcie umowy pożyczki), dla którego dane zostały podane. Z uwagi na stwierdzone uchybienia w procesie przetwarzania danych, wobec spółki, jako administratora danych, zostało wszczęte postępowanie administracyjne we wskazanym zakresie, a następnie – wydana decyzja[40] nakazująca usunięcie wskazanych uchybień, w tym m.in. usunięcie danych, dla których cel przetwarzania został osiągnięty. Spółka złożyła wniosek o ponowne rozpatrzenie sprawy podnosząc m.in., że podstawą przetwarzania danych osób, z którymi nie

[38] Decyzja DIS/DEC-1219/14/103025.
[39] Kontrola DIS-K-421/41/14.
[40] DIS/DEC-650/14/51215

została zawarta umowa, była zgoda na przesyłanie informacji handlowych dotyczących produktów oferowanych przez spółkę za pomocą środków komunikacji elektronicznej. Oceniając ponownie całokształt zebranego materiału dowodowego w przedmiotowej sprawie, Generalny Inspektor utrzymał w mocy zaskarżoną decyzję[41], wskazując m.in., że zgoda na przesyłanie informacji handlowej, o której mowa w art. 10 w zw. z art. 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 z późn. zm.) i zgoda na przetwarzanie danych osobowych powinny być wyrażone jako odrębne oświadczenia. W przeciwnym wypadku zachodziłaby sytuacja domniemania zgody z oświadczenia woli innej treści.

2.2.4. Służba zdrowia.

W okresie sprawozdawczym w podmiotach należących do sektora służby zdrowia zostało przeprowadzonych **18 kontroli**, w tym 14 kontroli[42] przeprowadzono w podmiotach prowadzących hurtownie farmaceutyczne oraz podmiotach prowadzących przynajmniej jeden z rodzajów działalności: pełnienie funkcji podmiotu odpowiedzialnego za lek, świadczenie usług w zakresie promocji produktów leczniczych i wyrobów medycznych, produkcja wyrobów medycznych. Wskazane kontrole miały na celu ustalenie, czy ww. podmioty pozyskują zeskanowane recepty od aptek, do których dostarczają produkty lecznicze i przetwarzają dane osobowe zawarte na tych receptach

Jak ustalono w toku przeprowadzonych kontroli, jedna z hurtowni farmaceutycznych pozyskiwała na zlecenie innej hurtowni farmaceutycznej (również objętej kontrolą) zanonimizowane kopie recept, zawierające wyłącznie: numer recepty, datę jej wystawienia oraz nazwę zamawianego leku. Informacje zawarte w zanonimizowanych kopiach recept były pozyskiwane w celu weryfikacji istnienia zapotrzebowania na lek po stronie pacjenta, w związku z ciążącym na hurtowni farmaceutycznej, jako podmiocie zajmującym się hurtowym obrotem produktami leczniczymi, obowiązkiem zapewnienia, w celu zabezpieczenia pacjentów, nieprzerwanego zaspokajania zapotrzebowania podmiotów uprawnionych do obrotu detalicznego produktami leczniczymi i przedsiębiorców zajmujących się obrotem hurtowym produktami leczniczymi, w ilości odpowiadającej potrzebom pacjentów, wynikającym z art. 36z ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne (Dz. U. z 2008 r. Nr 45, poz. 271 z późn. zm.).

---

[41] DIS/DEC-912/14/72496

[42] Np. kontrole DIS-K-421-130/14, DIS-K-421/145/14, DIS-K-421/157/14 i DIS-K-421/168/14.

Analiza przepisów ustawy Prawo farmaceutyczne oraz przepisów rozporządzenia Ministra Zdrowia z dnia 8 marca 2012 r. w sprawie recept lekarskich (Dz. U. z 2014 r., poz. 319 z późn. zm.) prowadzi do wniosku, że skoro prawo określa krąg podmiotów uprawnionych do dostępu do danych zawartych w receptach lekarskich, żaden inny podmiot (w tym poddany kontroli podmiot) posiadając dane w zakresie: numer recepty, data jej wystawienia oraz nazwa leku, nie będzie w stanie zidentyfikować osób, których te informacje dotyczą. W konsekwencji, należy przyjąć, że do przetwarzania przez spółkę danych w zakresie: numer recepty, data jej wystawienia oraz nazwa leku, nie znajdują zastosowania przepisy o ochronie danych osobowych.

Kontrola przeprowadzona w innym podmiocie wykazała z kolei, iż nie występował on z żądaniem przesłania kopii bądź skanów recept do podmiotów składających zamówienia na dany produkt leczniczy bądź wyrób medyczny. Zdarzały się jednak przypadki, iż do podmiotu wpływały skany bądź kopie recept, które mogły zawierać dane osobowe pacjentów bądź lekarzy, wówczas zgodnie z obowiązującą w podmiocie procedurą były one niezwłocznie usuwane.

Jak ustalono w toku kontroli przeprowadzonej w innym z podmiotów, zdarzały się przypadki, że wraz z formularzem zakupu interwencyjnego, apteki z własnej inicjatywy do tego podmiotu przesyłały skany bądź kopie recept. Ustalono, że na około 12000 wiadomości przesłanych drogą elektroniczną, które wpłynęły do podmiotu w 2014 r. i dotyczyły zakupów interwencyjnych miały miejsce tylko dwa przypadki nieskutecznego usunięcia skanów recept zawierających dane osobowe. W wyniku kontroli GIODO podmiot podjął działania mające na celu zapobieżenie otrzymywaniu skanów bądź kopii recept (w przypadku ich otrzymania - nieprzechowywania), poprzez aktualizację stosownych procedur, przeprowadzenie szkoleń oraz modyfikację formularza zakupu interwencyjnego.

2.2.5. Oświata.

W 2013 r. w placówkach oświatowych przeprowadzonych zostało **11 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Dziewięć z tych kontroli dotyczyło szkół wyższych[43].

Kontrole przeprowadzone w szkołach wyższych obejmowały przetwarzanie danych osobowych w związku z funkcjonowaniem domów studenckich szkół wyższych, w

[43] np. DIS-K-421/60/14, DIS-K-421/61/14, DIS-K-421/65/14, DIS-K-421/66/14, DIS-K-421/67/14, DIS-K-421/75/14, DIS-K-421/78/14.

szczególności: ubieganiem się o miejsca w domach studenckich, rozdziałem miejsc, zakwaterowaniem i wykwaterowaniem mieszkańców, odwiedzinami u mieszkańców.

Na podstawie dokonanych ustaleń stwierdzono, iż większość kontrolowanych uczelni w związku z rozdziałem miejsc oraz kwaterowaniem mieszkańców w domach studenckich zbiera dane osobowe w zakresie adekwatnym do celów ich przetwarzania. Kontrole wykazywały również, że uczelnie zastosowały środki techniczne i organizacyjne zapewniające ochronę danych osobowych, przetwarzanych w systemie tradycyjnym (papierowym), odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w szczególności dane osobowe zostały zabezpieczone przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W toku przeprowadzonych kontroli stwierdzono przypadki kwaterowania w domach studenta niektórych uczelni osób niebędących studentami (np.: gości studentów przedłużających pobyt w domu studenckim, a także „tzw. gości hotelowych") i wystawiania faktur VAT za taki pobyt. Ustalono, iż w związku z takim kwaterowaniem uczelnie jako administratorzy danych osobowych, pomimo iż przetwarzają dane osobowe ww. osób w zbiorach danych osobowych, nie zgłaszały takich zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, gdyż – jak sądziły - dane zawarte w tych zbiorach są przetwarzane wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej (przesłanka zwalniająca z obowiązku rejestracji zbioru danych osobowych, o której mowa w art. 43 ust. 1 pkt 8 ustawy o ochronie danych osobowych).

Generalny Inspektor nie zgodził się z powyższą opinią. Określony w taki sposób cel przetwarzania danych ww. osób może nie być przecież jedynym celem przetwarzania tych danych. Uczelniom mogą bowiem przysługiwać wobec takich osób roszczenia o naprawienie szkody w przypadku zniszczenia przez te osoby pokoju lub jego wyposażenia, a tym osobom roszczenia związane z nienależytym wykonaniem usługi. Przetwarzanie danych osobowych w sytuacji wystąpienia takich roszczeń następuje już w innym celu niż wystawienie faktury, rachunku lub prowadzenie sprawozdawczości finansowej, co oznacza w konsekwencji brak zwolnienia z obowiązku zgłoszenia tego zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Zastrzeżenia inspektorów wzbudziły także obowiązujące we wszystkich dziewięciu kontrolowanych uczelniach wewnętrzne procedury, które dopuszczały możliwość zatrzymywania dowodów osób odwiedzających mieszkańców domów studenckich przez

pracowników uczelni, co może prowadzić do naruszania w tym zakresie powszechnie obowiązujących przepisów prawa (art. 33 ustawy o ewidencji ludności i dowodach osobistych)[44]. Cele związane z zapewnieniem bezpieczeństwa na terenie domów studenckich i kontrolą ruchu osobowego w domu studenckim nie uzasadniają zastanej w toku kontroli praktyki zatrzymywania dokumentów należących do osób odwiedzających, ponieważ ich realizację zapewniać może prowadzona w domach studenckich ewidencja gości.

Pozostałe stwierdzone w toku kontroli uchybienia dotyczyły nieprawidłowości w systemach informatycznych (w tym niezapewnianie przez te systemy, dla każdej osoby, której dane osobowe są przetwarzane w tym systemie, odnotowania daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu, źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą), wymaganej przepisami o ochronie danych osobowych dokumentacji (np. braku ewidencji osób upoważnionych do przetwarzania danych osobowych), niezrealizowaniu obowiązku informacyjnego oraz niezapewnieniu możliwości swobodnego podjęcia decyzji o udzieleniu/odmowie udzielenia zgody na udostępnienie danych osobowych.

Wobec podmiotów, w których stwierdzono uchybienia dające podstawę do zastosowania środków, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych, wszczęte zostały postępowania administracyjne i wydane zostały decyzje nakazujące[45] usunięcie uchybień oraz decyzje umarzające[46] postępowanie, w sytuacji gdy nieprawidłowości usunięte zostały w toku prowadzonych postępowań.

2.2.6. Telekomunikacja.

W okresie sprawozdawczym u dostawców usług telekomunikacyjnych oraz w podmiotach współpracujących z dostawcami usług telekomunikacyjnych, przeprowadzonych zostało **6 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych[47].

W toku kontroli[48], której poddano spółkę telekomunikacyjną, na skutek zawiadomienia dotyczącego incydentu naruszeniu bezpieczeństwa danych osobowych, które zostało

---

[44] Art. 33. Dowodu osobistego nie wolno zatrzymywać, z wyjątkiem przypadków określonych w ustawie.

[45] np. DIS/DEC/1074/14/87541, DIS/DEC-1029/14/85027, DIS/DEC-1147/14/95831, DIS/DEC-916/14/72987.

[46] np. DIS/DEC-1117/14/92376, DIS/DEC-1028/14/85023, DIS/DEC1118/14/92381, DIS/DEC-1026/14/84765.

[47] Np. kontrole DIS-K-421/98/14 i DIS-K-421/138/14.

[48] DIS-K-421/27/14

zgłoszone Generalnemu Inspektorowi na podstawie art. 174a ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)[49] przez inną spółkę telekomunikacyjną, ustalono, iż ww. naruszenie bezpieczeństwa danych polegało na nieuprawnionym skopiowaniu w celu osiągnięcia korzyści majątkowej bazy danych klientów spółki kontrolowanej przetwarzanych w systemie informatycznym. Następnie doszło do ujawnieniu danych osobie trzeciej, co stanowiło działanie na niekorzyść spółki. Zachodziło zatem podejrzenie, iż osoba ta wykorzystała uprawnienia przyznane jej w związku z realizacją zadań służbowych w sposób niezgodny z umową i z naruszeniem przepisów karnych zawartych w art. 51 ust. 1 ustawy o ochronie danych osobowych[50], co stanowiło także naruszenie wewnętrznych procedur spółki.

Przeprowadzona kontrola wykazała jednocześnie, iż spółka jako administrator danych osobowych, stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych swoich klientów odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności spółka opracowała i wdrożyła procedury mające na celu zapewnienie ochrony danych osobowych przetwarzanych przez kontrolowany podmiot. Spółka, mając świadomość możliwości zaistnienia naruszeń przepisów wewnętrznych, w tym dotyczących ochrony danych osobowych, opracowała również procedury określające sposób reakcji w przypadku zaistnienia ww. naruszeń.

W związku ze stwierdzeniem, iż spółka w należyty sposób zabezpiecza dane osobowe, brak było podstaw do wszczęcia w przedmiotowej sprawie postępowania administracyjnego. Ze względu zaś na skierowanie przez spółkę do organów ścigania zawiadomienia o podejrzeniu popełnienia przestępstwa, niecelowe było również, aby Generalny Inspektor podejmował w przedmiotowej sprawie działania wskazane w art. 19 ustawy o ochronie danych osobowych[51].

---

[49] 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.

[50] Art. 51 ust. 1. 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.

[51] Art. 19. 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.

2.2.7. Zatrudnienie.

Jedną z ciekawszych kontroli przeprowadzonych w 2014 r. dotyczących zagadnień z zakresu zatrudnienia, była kontrola przeprowadzona w związku ze skargą związku zawodowego[52]. Zakresem przedmiotowej kontroli objęto przetwarzanie danych osobowych pracowników przebywających na terenie zakładu pracy, zarejestrowanych za pomocą urządzenia technicznego służącego do zapisu obrazu. Analiza materiału dowodowego zebranego w sprawie wykazała, iż kontrolowana jednostka w systemie informatycznym przetwarza nie tylko dane osobowe pracowników, ale także dane osobowe osób trzecich (tj. niebędących jej pracownikami). Utrwalone w ten sposób dane osobowe tworzą zestaw danych dostępnych według określonych kryteriów, a więc stanowiących zbiór danych osobowych, w rozumieniu art. 7 ust. 1 ustawy o ochronie danych osobowych[53], podlegający zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (art. 40 ustawy o ochronie danych osobowych[54]). Zgodnie bowiem z art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych[55], z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych m.in. w związku z zatrudnieniem u nich. Natomiast w odniesieniu do osób trzecich nie zachodzi żadna z okoliczności wskazanych w art. 43 ust. 1 ustawy o ochronie danych osobowych, zwalniających kontrolowaną jednostkę z obowiązku zgłoszenia do rejestracji wskazanego zbioru danych. Wobec powyższego wobec podmiotu poddanego kontroli w omawianym zakresie zostało wszczęte postępowanie administracyjne zakończone wydaniem decyzji administracyjnej. Kontrolowana jednostka wykonała nakaz decyzji w zakresie zgłoszenia do rejestracji Generalnemu Inspektorowi zbioru danych, w którym przetwarzane są dane osób trzecich zarejestrowanych za pomocą urządzenia służącego do rejestracji obrazu.

Do istotnych należała również kontrola przeprowadzonej w jednej ze spółek, do której kierowani są przez agencje pracy tymczasowej pracownicy tymczasowi[56]. Na podstawie materiału dowodowego zgromadzonego w sprawie ustalono, że poddana kontroli spółka

[52] Kontrola DIS-K-421/89/14.

[53] Art. 7 pkt 1. Przez zbiór danych rozumie się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

[54] Art. 40. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a.

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

[56] Kontrola DIS-K-421/88/14.

bezpośrednio od tych osób pozyskiwała dane osobowe w zakresie: imię i nazwisko, data urodzenia, obywatelstwo, miejsce zamieszkania, a także imię, nazwisko, adres i nr telefonu osoby, którą należy zawiadomić w razie wypadku. Spółka pozyskiwała od ww. osób zgodę w formie oświadczenia zamieszczonego w treści kwestionariusza osobowego dla pracownika tymczasowego.

Jak stwierdzono w wyniku przeprowadzenia analizy przepisów ustawy z dnia 9 lipca 2003 r. o zatrudnieniu pracowników tymczasowych (Dz. U. Nr 166, poz. 1608 z późn. zm.), w szczególności jej art. 14[57], przepisy te nie stanowią samodzielnej przesłanki przetwarzania danych osobowych pracowników tymczasowych przez spółkę. Nie określają bowiem zakresu danych osobowych pracowników tymczasowych, do których przetwarzania spółka (jako „pracodawca użytkownik"[58]) jest uprawniona w związku z koniecznością zapewnienia im bezpiecznych i higienicznych warunków pracy oraz prowadzenia ewidencji czasu pracy. Ustawodawca nie wskazał katalogu danych osobowych, który może być przetwarzany w odniesieniu do tej kategorii osób, a jedynie niektóre z możliwych celów przetwarzania danych. W toku kontroli ustalono, że spółka przetwarzała dane osobowe pracowników tymczasowych zarówno w celach określonych w powołanym wyżej przepisie, jak również w innych celach, np. kontroli realizacji zleceń produkcyjnych i rozliczenia czasu pracy na zlecenia produkcyjne wykonane przez pracownika tymczasowego. W konsekwencji uznano, iż spółka legitymuje się podstawą prawną przetwarzania danych osobowych pracowników tymczasowych wynikającą z art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, tj. zgodą osoby, której dane dotyczą, w związku z art. 23 ust. 1 pkt 2 tej ustawy[59], tj. korzysta z uprawnień określonych w ustawie o zatrudnieniu pracowników tymczasowych.

Jednocześnie Generalny Inspektor uznał, że zbiór danych osobowych pracowników tymczasowych prowadzony przez spółkę zwolniony jest z obowiązku rejestracji na podstawie art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych, zgodnie z którym, z obowiązku

---

[57] Art. 14 ust. 1. Pracodawca użytkownik wykonuje obowiązki i korzysta z praw przysługujących pracodawcy, w zakresie niezbędnym do organizowania pracy z udziałem pracownika tymczasowego. 2. Pracodawca użytkownik jest obowiązany zapewnić pracownikowi tymczasowemu bezpieczne i higieniczne warunki pracy w miejscu wyznaczonym do wykonywania pracy tymczasowej, prowadzi ewidencję czasu pracy pracownika tymczasowego w zakresie i na zasadach obowiązujących w stosunku do pracowników, nie może stosować do pracownika tymczasowego przepisu art. 42 § 4 Kodeksu pracy ani też powierzać mu do wykonania pracy na rzecz i pod kierownictwem innego podmiotu.

[58] Art. 2 pkt 1. Pracodawca użytkownik – pracodawca lub podmiot niebędący pracodawcą w rozumieniu Kodeksu pracy wyznaczający pracownikowi skierowanemu przez agencję pracy tymczasowej zadania i kontrolujący ich wykonanie.

[59] Art. 23 ust. 1 pkt 2. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to konieczne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych w związku z zatrudnieniem u nich.

2.2.8. Transport.

W okresie sprawozdawczym w podmiotach należących do tego sektora przeprowadzono **16 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych, w tym 13 kontroli przeprowadzono u przewoźników w związku z rezerwacją i zakupem biletów na przejazd (przewóz)[60].

Kontrolami przeprowadzonymi u przewoźników w związku z rezerwacją i zakupem biletów na przejazd (przewóz) objęto siedmiu przewoźników w transporcie drogowym, trzech przewoźników w transporcie kolejowym, jednego armatora prowadzącego transport pasażerski morski i przybrzeżny oraz dwa podmioty nie będące przewoźnikami, pośredniczące w sprzedaży biletów na przejazd w transporcie drogowym.

W toku jednej z kontroli ustalono, iż podmiot, który nie jest przewoźnikiem (nie prowadzi działalności w zakresie przewozu osób lub rzeczy), na podstawie umów agencyjnych zawartych z przewoźnikami świadczy na rzecz tych przewoźników usługi polegające na pośrednictwie w sprzedaży biletów na przewóz autokarami w ramach licencjonowanych linii w międzynarodowym transporcie drogowym. Jak wynika z zawartych umów agencyjnych podmiot ten opracowuje i wdraża system sprzedaży biletów, prowadzi systemy centralnej rezerwacji miejsc, rozpatruje reklamacje, nadzoruje i monitoruje sieci sprzedaży oraz udostępniania dane statystyczne dotyczące prowadzonej sprzedaży biletów na rzecz danego przewoźnika. Usługi, o których mowa powyżej, są wykonywane przez ten podmiot za pośrednictwem Internetu (strony internetowej tego podmiotu) oraz za pośrednictwem agentów, z którymi podmiot ten zawarł umowy agencyjne. W umowach agencyjnych zawartych z przewoźnikami znalazło się postanowienie zezwalające pośrednikowi na korzystanie z usług podwykonawców przy wykonywaniu usług zleconych przez przewoźników. W toku przedmiotowej kontroli pośrednik wskazał, iż podstawą prawną przetwarzania przez niego danych pozyskiwanych w związku z rezerwacją i sprzedażą biletów na przewóz stanowi art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych, tj. przetwarzanie danych jest niezbędne w celu realizacji umowy dotyczącej usługi organizacji przewozu zawartej pomiędzy pośrednikiem a klientem (przewoźnikiem). Natomiast dowodem

[60] Np. kontrole DIS-K-421/113/14, DIS-K-421/114/14, DIS-K-421/116/14, DIS-K-421/117/14, DIS-K-421/123/14, DIS-K-421/125/14, DIS-K-421/128/14.

zawarcia takiej umowy jest bilet na przejazd. W związku z powyższym uznano, że pośrednik przetwarza dane osobowe w związku z rezerwacją i sprzedażą biletów na przewóz autokarami, jako podmiot, któremu przewoźnicy powierzyli przetwarzanie danych osobowych w myśl art. 31 ustawy o ochronie danych osobowych, na podstawie zawartych umów agencyjnych. A tym samym administratorem danych[61] osób rezerwujących i kupujących bilety za pośrednictwem tego podmiotu są przewoźnicy. Skoro wiec przewoźnicy zawierając umowy z pośrednikiem decydowali, o celach i środkach przetwarzanych danych osób, o których mowa powyżej to przewoźników uznano za administratorów danych osób korzystających z usług przewozowych. Natomiast pośrednik błędnie uznał się za administratora danych osób korzystających z usług przewozowych, o czym świadczyło zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych zbioru danych klientów.

Ustalono także, że jeden z przewoźników, korzystający z dopłat do przewozów osób uprawnionych ustawowo do bezpłatnych lub ulgowych przejazdów środkami publicznego transportu zbiorowego autobusowego korzysta z ww. dopłat na podstawie umowy zawartej z marszałkiem województwa. W umowie tej opisane zostały zasady dotyczące przekazywania przewoźnikowi dopłat, o których mowa powyżej. Z postanowień przedmiotowej umowy wynika, że każdy sprzedany bilet miesięczny z ulgą ustawową 49% oraz 51% musi posiadać wpisany numer ewidencyjny PESEL osoby ustawowo uprawnionej do przejazdu na podstawie tego biletu. Odnosząc się do powyższego postanowienia umowy Generalny Inspektor zwrócił uwagę, iż drukowanie na bilecie miesięcznym numerów PESEL jego użytkownika, a także wykorzystywanie nr PESEL dla celów kontroli biletów miesięcznych narusza zasadę adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy. Albowiem zakres danych zapisanych na bilecie miesięcznym powinien być adekwatny do celów przetwarzania tych danych, tj. weryfikacji, czy biletem posługuje się osoba upoważniona do jego używania oraz kontroli, czy posiada ona uprawnienie do ulgi wskazanej na tym bilecie. Mając powyższe na uwadze w ocenie Generalnego Inspektora Ochrony Danych Osobowych drukowanie na bilecie miesięcznym nr PESEL jego użytkownika jako informacji niezbędnej do realizacji wskazanych powyżej celów nie znajduje uzasadnienia. W opisanym przypadku dane wystarczające do osiągnięcia ww. celów stanowią bowiem: imię i nazwisko, adres zamieszkania, numer dokumentu tożsamości (dowodu osobistego w przypadku biletu

[61] Art. 7 pkt 4. Ilekroć w ustawie jest mowa o administratorze danych rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę decydujące o celach i środkach przetwarzania danych osobowych.

normalnego) lub dokumentu potwierdzającego uprawnienie do ulgi ustawowej (w przypadku biletu ulgowego). W przedmiotowej sprawie niniejsza kwestia nie została objęta zakresem postępowania administracyjnego, gdyż w toku kontroli nie stwierdzono, by zaczęto pozyskiwać numery PESEL w ww. celu przez podmiot kontrolowany. Niemniej jednak Generalny Inspektor przedstawił przewoźnikowi swoje stanowisko, aby w przyszłości nie doszło do naruszenia przepisów o ochronie danych osobowych.

Na podstawie dokonanych ustaleń w toku kontroli przewoźników należy stwierdzić, iż kontrolowane podmioty nie zawsze zapewniały w sposób należyty bezpieczeństwo danych przesyłanych przy użyci środków komunikacji elektronicznej, gdyż nie w każdym przypadku stosowano środki kryptograficzne przy przekazywaniu danych osobowych przy wykorzystaniu publicznych sieci telekomunikacyjnych. Ponadto, nie wszystkie systemy informatyczne służące do przetwarzania danych osobowych użytkowane w podmiotach kontrolowanych posiadały funkcjonalności umożliwiające odnotowanie informacji, o których mowa w § 7 ust. 1 pkt 1 i 2 rozporządzenia, tj. daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

Niektóre podmioty kontrolowane miały problemy z prawidłowym wykonaniem podstawowych obowiązków określonych w przepisach o ochronie danych osobowych. Nieprawidłowości te najczęściej dotyczyły niedopełnienia obowiązku zgłoszenia prowadzonych zbiorów do rejestracji Generalnemu Inspektorowi. Sporadycznie stwierdzono inne uchybienia w procesie przetwarzania danych osobowych, np. nieliczni przewoźnicy zbierali dane osobowe w zakresie nieadekwatnym do celu ich przetwarzania, nie dopełnili obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy o ochronie danych. Niektóre uchybienia dotyczyły braku wymaganych elementów w dokumentacji opisującej sposób przetwarzania danych, tj.: polityce bezpieczeństwa, instrukcji zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych, gdyż nie zawierały elementów określonych w § 4 i § 5 rozporządzenia. W przypadku dwóch z kontrolowanych przewoźników stwierdzono powierzenie przetwarzania danych osobowych innym podmiotom bez zawarcia umowy powierzenia (art. 26 ust. 1 pkt 1 oraz art. 31 ust. 1 ustawy o ochronie danych osobowych).

Ponadto, w niektórych podmiotach wskazano na nieprawidłową treści klauzul zgód zamieszczonych na formularzu zamówienia biletów (dowodów przewozu). Zastrzeżenia budziła konstrukcja klauzul zgód, w ramach których umieszczonych zostało kilka oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych w różnych celach. Klauzule te nie

umożliwiały osobom, których dane dotyczą, dokonania swobodnego wyboru oraz wyrażenia zgody na przetwarzanie danych osobowych, bowiem osoby te nie miały możliwości podjęcia decyzji, w jakim celu udzielają zgody na przetwarzanie swoich danych osobowych, np. klauzula zgody na przetwarzanie danych osobowych zawartych w formularzu zamówienia nie została wyodrębniona od treści oświadczenia o zapoznaniu się z regulaminem przewozu.

Wobec podmiotów, w których stwierdzono uchybienia dające podstawę do zastosowania środków, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych, wszczęte zostały postępowania administracyjne, które zakończyły się wydaniem decyzji administracyjnych nakazujących[62] przywrócenie stanu zgodnego z prawem lub decyzji umarzających[63] postępowanie, jeżeli uchybienia objęte zakresem tego postępowania zostały usunięte w jego toku.

Oprócz opisanych wyżej kontroli sektorowych przewoźników, w 2014 r. w związku z docierającymi do Biura Generalnego Inspektor Ochrony Danych Osobowych sygnałami dotyczącymi możliwych nieprawidłowości w procesie przetwarzania danych osobowych na potrzeby realizowanego przez Prezydenta m.st. Warszawy projektu „Karta Warszawiaka" i „Karta Młodego Warszawiaka, w ramach którego wprowadzono uprawnienia do uzyskania zniżek lub ulg przy zakupie biletów komunikacji miejskiej, jak również możliwość korzystania z obiektów użyteczności publicznej m.st. Warszawy za opłatą obniżoną w stosunku do opłaty obowiązującej w tych obiektach dla osób spełniających kryteria określone w uchwałach Rady m.st. Warszawy, przeprowadzone zostały kontrole zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w: Zarządzie Transportu Miejskiego z siedzibą w Warszawie[64], w Urzędzie Miasta Stołecznego Warszawy[65] oraz w Ministerstwie Finansów[66].

W toku kontroli przeprowadzonej w Zarządzie Transportu Miejskiego z siedzibą w Warszawie (ZTM w Warszawie) ustalono, że przed rozpoczęciem procesu zbierania wniosków o wydanie Karty Warszawiaka lub Karty Młodego Warszawiaka, ZTM w Warszawie, jako administrator danych, udostępnił Prezydentowi m.st. Warszawy dane osobowe posiadaczy spersonalizowanej Warszawskiej Karty Miejskiej (funkcjonującej w warszawskich środkach komunikacji miejskiej), będących w przedziale wiekowym od 18 do

[62] Np. decyzje DIS/DEC-1077/14/87970 i DIS/DEC-37/15/4867.
[63] Np. decyzja DIS/DEC-1183/14/99494.
[64] Kontrola DIS-K-421/3/14.
[65] Kontrola DIS-K-421/10/14.
[66] Kontrola DIS-K-421/11/14.

70 lat, na potrzeby ww. projektu. Dane te pochodziły ze zbioru danych o nazwie „Spersonalizowane Warszawskie Karty Miejskie" (nr księgi rejestrowej: 087939) i zostały przekazane Prezydentowi m.st. Warszawy w celu przeprowadzenia weryfikacji uprawnień osób, których dane dotyczą, umożliwiających otrzymanie Karty Warszawiaka lub Karty Młodego Warszawiaka. Dane przekazano pomimo, iż osoby, których dane dotyczą, nie wyrażały zgody na przetwarzanie danych osobowych w ww. celu, a ponadto nie była spełniona żadna z pozostałych przesłanek legalizujących przetwarzanie danych osobowych (art. 23 ust. 1 ustawy o ochronie danych osobowych).

Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące prawo[67] Generalny Inspektor Ochrony Danych Osobowych uznał, że Zarząd Transportu Miejskiego z siedzibą w Warszawie udostępnił Prezydentowi m.st. Warszawy dane osobowych posiadaczy spersonalizowanej Warszawskiej Karty Miejskiej do przetwarzania na potrzeby projektu Karta Warszawiaka i Karta Młodego Warszawiaka bez podstawy prawnej.

W związku z powyższym Generalny Inspektor wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. W toku postępowania przedmiotowe uchybienie w procesie przetwarzania danych osobowych zostało usunięte, tj.: ZTM w Warszawie zaprzestał udostępniania Prezydentowi m.st. Warszawy danych osobowych posiadaczy spersonalizowanej Warszawskiej Karty Miejskiej ze zbioru danych o nazwie „Spersonalizowane Warszawskie Karty Miejskie" (nr księgi rejestrowej: 087939) na potrzeby projektu Karta Warszawiaka i Karta Młodego Warszawiaka. Z powyższych względów Generalny Inspektor Ochrony Danych Osobowych umorzył postępowanie w niniejszej sprawie.

---

[67] 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, z zastrzeżeniem ust. 2; zgodnie z ust. 2, przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje: 1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, 2) z zachowaniem przepisów art. 23 i 25 ustawy. Art. 23 ust. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą, 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Art. 31 ust. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

W toku kontroli przeprowadzonej w Urzędzie Miasta Stołecznego Warszawy ustalono zaś, że dla celów realizacji projektu „Karta Warszawiaka" i „Karta Młodego Warszawiaka (weryfikacji uprawnień do otrzymania „Karty Warszawiaka" lub „Karty Młodego Warszawiaka) Prezydent m.st. Warszawy pozyskiwał dane osobowe ze zbioru Centralny Rejestr Podmiotów – Krajowa Ewidencja Podatników (CRP KEP) prowadzonego przez Ministra Finansów na podstawie ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2012 r. poz. 1314 z późn. zm.). W celu uzyskania danych z CRP KEP na potrzeby ww. projektu, Prezydent m.st. Warszawy kierował do Ministra Finansów zapytanie, czy dana osoba posiadała na dzień 31 grudnia roku poprzedzającego rok, w którym złożyła wniosek o hologram „Karta Warszawiaka" lub „Karta Młodego Warszawiaka", adres miejsca zamieszkania na terenie m.st. Warszawy. W tym celu podawał dane osobowe osób ubiegających się o wydanie „Karty Warszawiaka" lub „Karty Młodego Warszawiaka" w zakresie: imię, nazwisko, nr PESEL, a w przypadku cudzoziemców: imię, nazwisko, datę urodzenia oraz NIP. Z kolei Minister Finansów uzupełniał przekazane dane osobowe poprzez podanie informacji dotyczącej posiadania (lub nie) miejsca zamieszkania na terenie m.st. Warszawy.

Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące prawo, w szczególności biorąc pod uwagę art. 5 ustawy o ochronie danych osobowych oraz przepisy regulujące funkcjonowanie CRP KEP[68], Generalny Inspektor uznał, że Prezydent m.st.

[68] Art. 5. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw. Art. 14 ust. 1 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2012 r. poz. 1314 z późn. zm.). Minister właściwy do spraw finansów publicznych prowadzi w formie elektronicznej CRP KEP. Ust. 2 ww. ustawy. CRP KEP służy: 1) gromadzeniu wybranych danych ewidencyjnych z rejestru PESEL dotyczących osób fizycznych objętych tym rejestrem oraz danych wynikających: a) ze zgłoszeń identyfikacyjnych i aktualizacyjnych podmiotów, b) z niektórych dokumentów związanych z obowiązkami wynikającymi z przepisów podatkowych; 2) weryfikacji danych, o których mowa w pkt 1, oraz porównaniu ich z rejestrami urzędowymi prowadzonymi na podstawie odrębnych przepisów. Art. 15 ust. 2 ww. ustawy. Dane zgromadzone w CRP KEP udostępnia się wyłącznie: 1) sądom, prokuratorom, organom podatkowym, organom celnym, przedstawicielom Najwyższej Izby Kontroli, Policji, Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego i Żandarmerii Wojskowej - w związku z prowadzonym postępowaniem; 1a) Szefowi Krajowego Centrum Informacji Kryminalnych w celu realizacji jego zadań ustawowych; 1b) (uchylony); 1c) komornikom sądowym i organom egzekucyjnym wymienionym w odrębnych przepisach - w związku z prowadzonym postępowaniem egzekucyjnym lub zabezpieczającym; 2) naczelnym i centralnym organom administracji rządowej - w związku z postępowaniem w sprawie udzielenia koncesji bądź zezwolenia na prowadzenie działalności gospodarczej; 3) podatnikowi - w zakresie dotyczącym jego numeru; 4) służbom statystyki publicznej w zakresie i dla potrzeb wynikających z przepisów o statystyce publicznej; 5) Zakładowi Ubezpieczeń Społecznych oraz Państwowemu Funduszowi Rehabilitacji Osób Niepełnosprawnych - do realizacji zadań i celów określonych w odrębnych ustawach; 6) (uchylony); 7) organom prowadzącym urzędowe rejestry na podstawie odrębnych przepisów, na wniosek zawierający dane niezbędne do identyfikacji podmiotów, o których mowa w art. 2, w zakresie NIP, w związku z realizacją ich zadań ustawowych.

Warszawy nie jest uprawniony do pozyskiwania danych dotyczących zamieszkiwania (bądź nie) na terenie m.st. Warszawy z CRP KEP dla realizacji celu, jakim jest weryfikacja uprawnień do otrzymania hologramu „Karta Warszawiaka" lub „Karta Młodego Warszawiaka", a co za tym idzie, brak jest podstaw do udostępniania Ministrowi Finansów danych uczestników programu „Karta Warszawiaka" lub „Karta Młodego Warszawiaka" w celu pozyskania informacji o tych osobach z CRP KEP.

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych, wobec Prezydenta m.st. Warszawy zostało wszczęte postępowanie administracyjne, zakończone następnie decyzją Generalnego Inspektora z dnia 26 czerwca 2014 r., nr DIS-DEC-600/14/48641, nakazującą Prezydentowi Miasta Stołecznego Warszawy usunięcie uchybień w procesie przetwarzania danych osobowych, m.in. poprzez: zaprzestanie przekazywania danych osobowych osób ubiegających się o „Kartę Warszawiaka" lub „Kartę Młodego Warszawiaka" do Ministerstwa Finansów w celu dokonania weryfikacji w Centralnym Rejestrze Podmiotów - Krajowej Ewidencji Podatników, czy osoby te posiadały na dzień 31 grudnia roku poprzedzającego rok, w którym złożyły wniosek o hologram, adres miejsca zamieszkania na terenie m.st. Warszawy oraz zaprzestanie pozyskiwania danych osobowych z CRP KEP w celu weryfikowania uprawnień do otrzymania „Karty Warszawiaka" lub „Karty Młodego Warszawiaka". Pełnomocnik Prezydenta Miasta Stołecznego Warszawy złożył wniosek o ponowne rozpatrzenie sprawy zakończonej ww. decyzją Generalnego Inspektora Ochrony Danych Osobowych i uchylenie w części zaskarżonej decyzji oraz umorzenie postępowania w tym zakresie. Po dokonaniu ponownej analizy całokształtu materiału dowodowego zebranego w niniejszej sprawie, Generalny Inspektor Ochrony Danych Osobowych, decyzją z dnia 2 października 2014 r. nr DIS/DEC-964/14/77489, utrzymał w mocy zaskarżoną decyzję w zakresie nakazów dotyczących pozyskiwania danych z CRP KEP dla weryfikacji uprawnień do otrzymania hologramu „Karta Warszawiaka" lub „Karta Młodego Warszawiaka" oraz udostępniania danych uczestników programu „Karta Warszawiaka" lub „Karta Młodego Warszawiaka" Ministrowi Finansów w celu pozyskania informacji o tych osobach. W pozostałym zakresie uchylił zaskarżoną decyzję. W dniu 6 listopada 2014 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga Prezydenta Miasta Stołecznego Warszawy na decyzję Generalnego Inspektora Ochrony Danych Osobowych z dnia 2 października 2014 r., nr DIS/DEC-964/14/77489 w części utrzymującej w mocy decyzję z dnia 26 czerwca 2014 r., nr DIS/DEC-600/14/48641.

Natomiast kontrola przeprowadzona w Ministerstwie Finansów wykazała, że Minister Finansów, jako administrator danych, pomimo braku podstawy prawnej, udostępniał Prezydentowi m.st. Warszawy dane ze zbioru Centralny Rejestr Podmiotów – Krajowa Ewidencja Podatników, prowadzonego na podstawie ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2012 r. poz. 1314 z późn. zm.), w celu weryfikacji uprawnień do wydania „Karty Warszawiaka" lub „Karty Młodego Warszawiaka". Przepisy wskazanej ustawy nie dają podstawy do udostępnienia organowi samorządu terytorialnego danych osobowych podatników w celach, w jakich miały zostać wykorzystane przez Prezydenta m.st. Warszawy. W związku z powyższym, Generalny Inspektor wszczął z urzędu wobec Ministra Finansów postępowanie administracyjne w niniejszej sprawie. Następnie wydana została decyzja[69] nakazująca Ministrowi Finansów przywrócenie stanu zgodnego z prawem poprzez nieudostępnianie Prezydentowi m.st. Warszawy danych ze zbioru Centralny Rejestr Podmiotów – Krajowa Ewidencja Podatników w celu weryfikacji uprawnień do wydania „Karty Warszawiaka" lub „Karty Młodego Warszawiaka". Na skutek wniosku Ministra Finansów o ponowne rozpatrzenie sprawy, po dokonaniu ponownej analizy materiału dowodowego, Generalny Inspektor Ochrony Danych Osobowych utrzymał w mocy swoją decyzję. Minister Finansów złożył do Wojewódzkiego Sądu Administracyjnego skargę na ww. decyzje.

W toku kontroli prowadzonej w jednym z przedsiębiorstw transportu lotniczego[70] w zakresie zabezpieczenia danych osobowych pasażerów, którzy zakupili bilet lotniczy w serwisie internetowym tego przedsiębiorstwa przed ich udostępnieniem osobom nieupoważnionym, w tym udostępnieniem informacji o zakupie biletów innym pasażerom na adresy ich poczty elektronicznej ustalono, iż wskazane przedsiębiorstwo powierzyło wdrożenie systemu informatycznego, służącego do wywoływania usług w serwisie internetowym za pomocą, którego pasażerowie dokonują zakupu biletów lotniczych, innemu podmiotowi. Ustalenia wykazały, iż przedsiębiorstwo zawarło w tym podmiotem także umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych.

Kontrola wykazała, iż w celu usprawnienia procesu zakupu biletów lotniczych, skierowanego przede wszystkim do osób, które często dokonują zakupu tych biletów za pośrednictwem serwisu przedsiębiorstwa, została włączona w dniu 5 listopada 2013 r.

[69] Decyzja DIS/DEC-623/14/49897.
[70] Kontrola DIS-K-421/9/14.

przez ww. podmiot, któremu przedsiębiorstwo powierzyło wdrożenie systemu informatycznego, dodatkowa funkcja polegająca na automatycznym uzupełnianiu danych osobowych pasażera w formularzu zakupu biletu lotniczego zamieszczonym w serwisie internetowym. Użytkownicy, którzy założyli konto w serwisie, podając w wyniku zakładania tego konta adres poczty elektronicznej oraz dane osobowe w zakresie obejmującym co najmniej: imię, nazwisko i numer telefonu, w przypadku dokonywania zakupu biletu lotniczego, nie wprowadzają tych danych do formularza zakupu biletu. System informatyczny automatycznie wypełnia pola danymi podanymi wcześniej w wyniku zakładania konta (imię i nazwisko, numer telefonu). Użytkownik wprowadza jedynie informacje dotyczące np. miejsca, daty, godziny wylotu i przylotu, miejsca w samolocie.

Ustalenia wykazały, iż w wyniku włączenia funkcji automatycznego uzupełniania danych pasażera w formularzu zakupowym doszło do nieuprawnionego dostępu do danych jednego z pasażerów dokonującego zakupu biletu lotniczego przez innego pasażera również dokonującego zakupu. Niezwłocznie po zgłoszeniu incydentu przez pasażera, którego dane zostały udostępnione, przedsiębiorstwo zgłosiło incydent za pomocą systemu służącego do zgłaszania i śledzenia błędów w systemie informatycznym z priorytetem „krytyczny" podmiotowi wdrażającemu system informatyczny służący do wywoływania usług w serwisie internetowym. Po podjęciu działań zmierzających do usunięcia ww. nieprawidłowości, podmiot wdrażający system informatyczny zmodyfikował w ciągu dwóch godzin serwis informatyczny w ten sposób, iż dla każdego użytkownika przydzielony został unikalny odrębny identyfikator ID, który jednoznacznie identyfikuje tego użytkownika, nie tylko w serwisie informatycznym przedsiębiorstwa, ale także w systemie informatycznym służącym do rezerwacji biletów lotniczych oraz w systemie informatycznym służącym do opłaty za bilet lotniczy. Poprzednio dla każdego zalogowanego w serwisie użytkownika przydzielony był identyfikator systemu informatycznego, a nie odrębny dla tego użytkownika unikalny identyfikator ID.

Ponadto, w związku z jednorazowym incydentem dotyczącym dostępu do danych osobowych użytkownika (pasażera) przez innego pasażera, przedsiębiorstwo zleciło podmiotowi wdrażającemu system informatyczny przeprowadzenie testów penetracyjnych systemu – serwisu i wybranych funkcji procesu rezerwacyjnego. W wyniku tych testów nie stwierdzono podatności, które skutkują możliwością uzyskania nieuprawnionego dostępu do danych osobowych pasażerów przetwarzanych w serwisie – systemach informatycznych lub nieuprawnionego dostępu do infrastruktury informatycznej przedsiębiorstwa.

W związku z tym, iż dostęp do serwisu służącego do zakupu elektronicznego biletu lotniczego z wykorzystaniem systemem informatycznego posiadają wyłącznie zarejestrowani pasażerowie przedsiębiorstwa w celu sprawdzenia, czy system informatyczny zabezpieczony jest w procesie zakupu biletu przed innymi pasażerami, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych inspektorzy dokonali w toku kontroli oględzin systemu informatycznego z pozycji nowego użytkownika, poprzez przejście całego procesu rezerwacyjnego, tj. od momentu założenia przez użytkownika konta w serwisie do momentu zakupu przez niego biletu lotniczego. W wyniku tak dokonanych oględzin nie stwierdzono, - pasażer (użytkownik) posiadał dostęp do jakichkolwiek danych dotyczących innego pasażera.

Biorąc pod uwagę natychmiastowe działania podjęte przez kontrolowane przedsiębiorstwo oraz podmiot wdrażający w przedsiębiorstwie system informatyczny służący do wywoływania usług w serwisie internetowym, 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[71].

2.2.9. Usługi pocztowe.

Z inicjatywy Generalnego Inspektora Ochrony Danych Osobowych oraz na podstawie pism wpływających do Biura GIODO w 2014 r. przeprowadzono kontrole zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych u operatorów pocztowych i w podmiotach świadczących usługi pocztowe realizowane na rzecz organów władzy publicznej, w szczególności jednostek sądownictwa powszechnego i powszechnych jednostek organizacyjnych prokuratury.

Generalny Inspektor przeprowadził czynności kontrolne u trzech operatorów pocztowych[72], a także w dziewięciu wybranych oddziałach i punktach obsługi klienta[73] prowadzonych przez podmioty, które, jako podwykonawcy operatora pocztowego, wykonują w jego imieniu usługi pocztowe realizowane na rzecz jednostek organizacyjnych sądownictwa powszechnego i powszechnych jednostek organizacyjnych prokuratury.

---

[71] 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.

[72] Kontrole: DIS-K-421/49/14, DIS-K-421/28/14, DIS-K-421/90/14.

[73] Kontrole: DIS-K-421/30/14, DIS-K-421/32/14, DIS-K-421/39/14, DIS-K-421/38/14, DIS-K-421/47/14, DIS-K-421/52/14, DIS-K-421/53/14, DIS-K-421/54/14, DIS-K-421/55/14.

W toku przeprowadzonych kontroli ustalono, iż w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na świadczenie usług pocztowych zawarte zostały dwie odrębne umowy na świadczenie usług pocztowych w obrocie krajowym i zagranicznym pomiędzy spółką, będącą operatorem pocztowym a Skarbem Państwa - Sądem Apelacyjnym w Krakowie, a także Skarbem Państwa - Prokuratorem Generalnym. Przedmiotem wyżej wskazanych umów jest świadczenie przez ww. spółkę odpowiednio na rzecz jednostek organizacyjnych sądownictwa powszechnego oraz powszechnych jednostek organizacyjnych prokuratury, usług pocztowych w obrocie krajowym i zagranicznym w zakresie przyjmowania, przemieszczania i doręczenia przesyłek pocztowych oraz zwrotu przesyłek niedoręczonych. Świadczenie usług pocztowych przez spółkę na rzecz jednostek sądownictwa powszechnego, a także na rzecz powszechnych jednostek organizacyjnych prokuratury w zakresie wskazanym powyżej obejmuje przesyłki pocztowe (przesyłki listowe i przesyłki kurierskie) zarówno rejestrowane jak i nierejestrowane. Przesyłki pocztowe rejestrowane oznacza się inaczej jako przesyłki awizowane.

W toku kontroli ustalono, iż spółka świadczy usługi pocztowe realizowane na rzecz jednostek sądownictwa powszechnego i powszechnych jednostek organizacyjnych prokuratury korzystając z własnej infrastruktury technicznej i organizacyjnej oraz w ramach współpracy z podmiotami trzecimi. Spółka posiada własne punkty obsługi klienta oraz punkty obsługi klienta prowadzone przez podmioty zewnętrzne, z którymi zawarto umowy na ich prowadzenie. Umowy te zawierają – stosownie do art. 31 ustawy o ochronie danych osobowych, elementy określające cel i zakres danych osobowych powierzonych do przetwarzania podmiotowi prowadzącemu punkt obsługi klienta.

Generalny Inspektor uznał, iż w zakresie objętym kontrolą ww. operator pocztowy posiada status administratora danych, natomiast podmioty prowadzące oddziały agencyjne lub punkty obsługi klienta, z którymi operator zawarł stosowne umowy, przetwarzają dane osobowe na podstawie w art. 31 ust. 1 ustawy o ochronie danych osobowych.

Czynności kontrolne nie wykazały w zakresie objętym kontrolą uchybień w procesie przetwarzania danych osobowych przez ww. operatorów pocztowych świadczących usługi pocztowe (w zakresie przesyłek awizowanych) realizowanych na rzecz organów władzy publicznej, w szczególności jednostek sądownictwa powszechnego, a także na rzecz powszechnych jednostek organizacyjnych prokuratury. Natomiast stwierdzono uchybienia w oddziałach i punktach obsługi klienta prowadzonych przez podmioty, które jako

podwykonawcy operatora pocztowego wykonują usługi pocztowe realizowane m.in. na rzecz ww. jednostek.

Przeprowadzone kontrole wykazały, iż pięć z ww. podmiotów naruszyło przepisy ustawy o ochronie danych. Stwierdzone w toku kontroli uchybienia polegały na nieopracowaniu dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, niewyznaczeniu administratora bezpieczeństwa informacji, nienadaniu pracownikom dopuszczonym do przetwarzania danych osobowych upoważnień, nieprowadzeniu ewidencji osób upoważnionych do przetwarzania danych osobowych, niezastosowaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności niezabezpieczeniu danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, polegające na niezabezpieczeniu danych osobowych odbiorców przesyłek przed ich udostępnieniem osobom nieupoważnionym, tj. osobom przebywającym na sali sprzedaży, do której wejście od strony magazynu nie było zabezpieczone drzwiami wyposażonymi w zamek.

Wobec tych podmiotów, które naruszyły przepisy o ochronie danych osobowych, wszczęte zostały postępowania administracyjne, które zakończyły się wydaniem decyzji administracyjnych nakazujących przywrócenie stanu zgodnego z prawem lub decyzji umarzających postępowanie, jeżeli uchybienia objęte zakresem tego postępowania zostały usunięte w jego toku.

2.2.10. Usługi hotelarskie.

W 2014 roku przeprowadzono **5 kontroli** w podmiotach prowadzących hotele[74]. Zakresem ww. kontroli objęto przetwarzanie przez te podmioty danych osobowych osób nieletnich, identyfikowanych wraz z osobami dorosłymi korzystającymi z usług hotelarskich tych hoteli. Przeprowadzone kontrole wykazały, iż pracownicy recepcji hotelowych, w przypadku gdy zauważą nieprawidłowości dotyczące sposobu zachowania gościa przebywającego w obiekcie wraz z osobą nieletnią polegające na wystąpieniu ewentualnego zagrożenia bezpieczeństwa dziecka (np. stosowanie wobec dziecka przemocy fizycznej bądź psychicznej, w tym wykorzystywania dziecka w celach seksualnych), zobowiązani są do poinformowania odpowiedniego kierownika bądź menedżera o takiej sytuacji, w celu

[74] Np. kontole DIS-K-421/155/14, DIS-K-421/161/14, DIS-K-421/166/14, DIS-K-421/167/14.

podjęcia decyzji o dalszym trybie postępowania, z uwzględnieniem konieczności zawiadomienia odpowiednich organów (Policji), urzędów lub instytucji. W skontrolowanych podmiotach nie było zdarzenia związanego z zagrożeniem bezpieczeństwa dziecka, w tym dotyczącego przemocy fizycznej bądź psychicznej, a także wykorzystywania w celach seksualnych. Czynności kontrolne przeprowadzone w podmiotach prowadzących hotele nie wykazały, w zakresie objętym kontrolą, uchybień w procesie przetwarzania danych osobowych, ponieważ nie stwierdzono przetwarzania danych osób nieletnich, przebywających wraz z osobami dorosłymi korzystającymi z usług hotelarskich.

2.2.11. Inne.

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

W związku z przedmiotem badań podgrupy ds. międzynarodowego przekazywania danych, działającej w ramach Grupy Roboczej Art. 29, w celu ustalenia praktyki w zakresie przekazywania danych osobowych związanych z działalnością agencji antydopingowych w państwach Europejskiego Obszaru Gospodarczego przeprowadzono cztery kontrole[75] zgodności przetwarzania danych z przepisami o ochronie danych osobowych w podmiotach przetwarzających dane osobowe w systemie informatycznym o nazwie „ADAMS" (Anti-Doping Administration & Management System). Kontrolami objęto dane osobowe zawodników przetwarzane w ww. systemie.

System informatyczny o nazwie „ADAMS" został stworzony w celu prowadzenia efektywnej polityki antydopingowej na całym świecie. Jest to elektroniczna baza danych dostępna online. Z ww. systemu korzystają międzynarodowe federacje sportowe oraz narodowe organizacje antydopingowe. „ADAMS" składa się z czterech podstawowych paneli: 1) baza danych zawierająca informacje o miejscach pobytu zawodników (Athletes Whereabouts) - elektroniczna baza danych pozwala zawodnikom na wprowadzanie informacji o ich miejscach pobytu drogą elektroniczną; dozwolone są również inne formy przekazu takie jak fax lub SMS; zawodnicy, którzy nie mają stałego dostępu do internetu mogą wyznaczyć przedstawiciela odpowiedzialnego za wprowadzanie aktualnych wpisów np. trener; analiza i wykorzystanie wprowadzonych danych pozwala na przeprowadzanie niespodziewanych kontroli antydopingowych poza zawodami, 2) forum wymiany informacji dla organizacji

[75] Kontrole DIS-K-421/4/14, DIS-K-421/12/14, DIS-K-421/20/14, DIS-K-421/21/14.

antydopingowych (Information Clearing House) - służące przechowywaniu wszystkich danych dotyczących wyników kontroli antydopingowych, wyłączeń dla celów terapeutycznych oraz informacji o naruszeniach przepisów antydopingowych; głównym celem tego panelu jest ułatwienie przepływu i wymiany informacji pomiędzy organizacjami antydopingowymi oraz zagwarantowanie przejrzystości polityki antydopingowej, 3) Platforma Kontroli Antydopingowych (Doping Control Platform) - pozwalająca na używanie systemu w celu planowania badań i analizy kontroli antydopingowych prowadzonych przez konkretną organizację antydopingową. Funkcja dostępna jest jedynie dla określonych organizacji antydopignowych, 4) Panel TUE (TUE Management) - pozwalający na zarządzanie wyłączeniami dla celów terapeutycznych oraz na przekazywanie ich odpowiednim organizacjom antydopingowym.

W świetle ustaleń dokonanych w toku kontroli uznano, iż administratorem danych osobowych przetwarzanych w systemie informatycznym o nazwie „ADAMS" jest światowa organizacja antydopingowa (w stosunku do danych osobowych wszystkich zawodników) oraz krajowa organizacja antydopingowa (w odniesieniu do danych osobowych polskich zawodników). Ponadto przyjęto, iż podstawą prawną do przetwarzania przez krajową organizację antydopingową danych osobowych zawodników w systemie ADAMS jest art. 44 ust. 5 pkt ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. Nr 127. poz. 857 z późn. zm.), zgodnie z którym krajowa organizacja antydopingowa ma prawo do przeprowadzania kontroli antydopingowych podczas zawodów oraz poza nimi. Jednocześnie ww. organizacja posiada dostęp do danych osobowych zawodników przetwarzanych w systemie „ADAMS", w związku z umową zawartą ze światową organizacją antydopingową w sprawie użytkowania i wymiany informacji zgromadzonych w systemie administrowania i zarządzania informacjami antydopingowymi „ADAMS" opracowanym i prowadzonym przez światową organizacją antydopingową.

Jednocześnie na podstawie wyników kontroli zostały wszczęte dwa postępowania administracyjne w zakresie stwierdzonych uchybień, które zakończyły się wydaniem przez Generalnego Inspektora – w jednym przypadku decyzji umarzającej[76] postępowanie administracyjne w zakresie stwierdzonych w toku kontroli uchybień, a w drugim decyzji nakazującej[77] przywrócenie stanu zgodnego z prawem poprzez dopełnienie przez krajową organizację antydopingową wobec polskich zawodników, których dane osobowe są

[76] Decyzja DIS/DEC-855/14/66893.
[77] Decyzje DIS/DEC-676/14/55359.

przetwarzane w systemie informatycznym o nazwie „ADAMS", obowiązku informacyjnego, o którym mowa w art. 24 ustawy o ochronie danych osobowych.

Do interesujących należała kontrola przeprowadzona w jednym ze stowarzyszeń[78]. Zakresem tej kontroli zostały objęte dane osobowe dzieci, rodziców i nauczycieli ze szkół – różnego stopnia edukacji – będących członkami i partnerami stowarzyszenia. Dane na podstawie zawartych przez to stowarzyszenie umów o współpracy, zostały udostępnione podmiotowi zewnętrznemu, w związku z dokonaniem przez ten podmiot cesji praw i obowiązków wynikających z powołanych umów innemu podmiotowi.

Przeprowadzona kontrola wykazała m.in., iż stowarzyszenie rozpoczęło realizację projektu, którego celem było stworzenie programu lojalnościowego dostępnego dla użytkowników portalu internetowego dedykowanego dla tego programu oraz stworzenie platformy sprzedaży on-line, służącej do zaopatrywania szkół i rodziców we wszystkie niezbędne artykuły potrzebne placówkom edukacyjnym oraz uczniom. Jak ustalono, w celu realizacji powyższego projektu stowarzyszenie pierwotnie podjęło współpracę z jednym z ww. podmiotów. Na podstawie umowy cesji – za zgodą i wiedzą stowarzyszenia – drugi z ww. podmiotów wszedł w prawa i obowiązki pierwszego z nich. Umowy o współpracy zawierały w swej treści m.in. postanowienia o udostępnieniu przez stowarzyszenie drugiej stronie umowy danych osobowych dzieci, rodziców i nauczycieli ze szkół będących członkami i partnerami stowarzyszenia. Ustalono jednak, iż stowarzyszenie nie przekazało ani nie udostępniło do wglądu ww. danych osobowych. Wskazane postanowienia zostały następnie zmienione na mocy aneksów. Wprowadzone zmiany polegały na wykreśleniu w każdej z ww. umów o współpracy postanowień, które dotyczyły zapewnienia przez stowarzyszenie drugiej stronie umowy dostępu do danych osobowych dzieci, rodziców i nauczycieli na potrzeby marketingowe i zastąpieniu go postanowieniem, zgodnie z którym jeden z podmiotów będzie mógł uzyskać bezpośredni dostęp do wykorzystania w działaniach marketingowych danych teleadresowych rodziców i nauczycieli, którzy wyrazili na to zgodę, będących członkami stowarzyszenia na dzień podpisania umowy oraz tych, którzy staną się członkami lub partnerami stowarzyszenia w tracie jej trwania. Pozostałe warunki umów pozostały bez zmian. Zatem zapewniono, aby dane osobowe rodziców i nauczycieli, których administratorem jest stowarzyszenie, były wykorzystywane w celach marketingowych przez spółkę jedynie w sytuacji, gdy osoby, których te dane dotyczą, wyraziły na to zgodę. Mając

[78] Kontrola DIS-K-421/97/14.

powyższe na uwadze stwierdzono, iż w zakresie objętym kontrolą stowarzyszenie nie narusza już przepisów o ochronie danych osobowych.

2.3. Systemy informatyczne służące do przetwarzania danych osobowych.

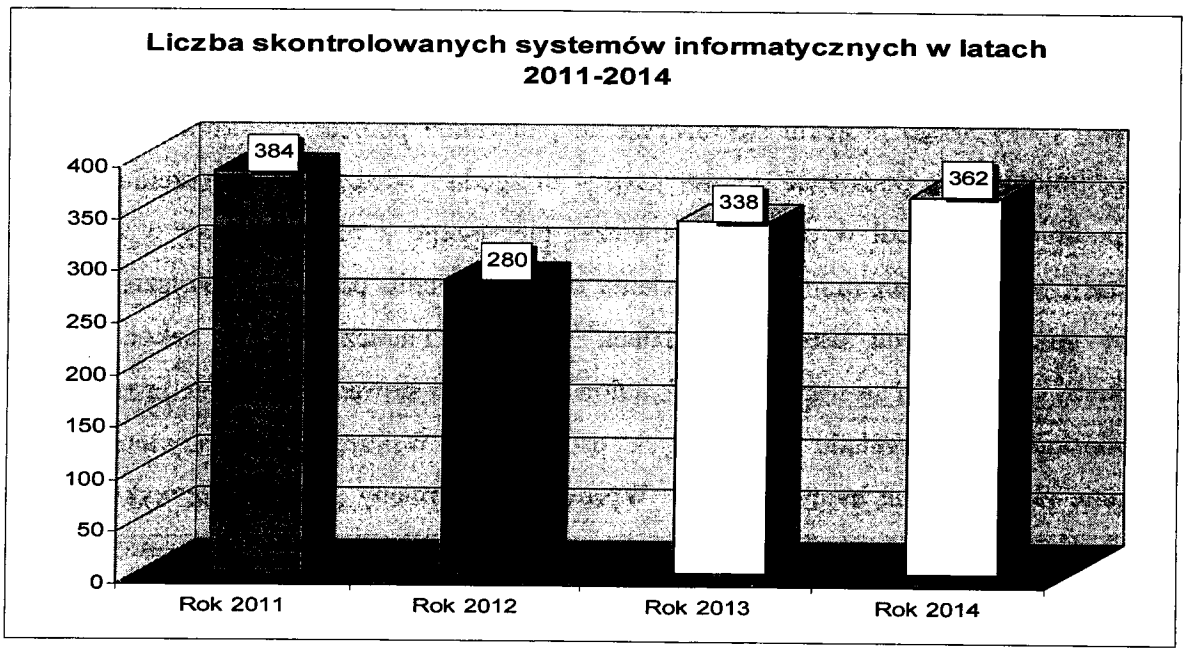
W ramach 175 przeprowadzonych w 2014 r. kontroli, weryfikacji poddano 362 systemy informatyczne wykorzystywane do przetwarzania danych osobowych.

rok 2011 = 188 kontroli, obejmujących 384 systemów informatycznych,

rok 2012 = 162 kontroli, obejmujących 280 systemy informatyczne.

rok 2013 = 165 kontroli, obejmujących 338 systemy informatyczne.

rok 2014 = 175 kontroli, obejmujących 368 systemy informatyczne.



Wykres 2: ***Zestawienie porównawcze liczby skontrolowanych systemów informatycznych w latach 2011-2014.***

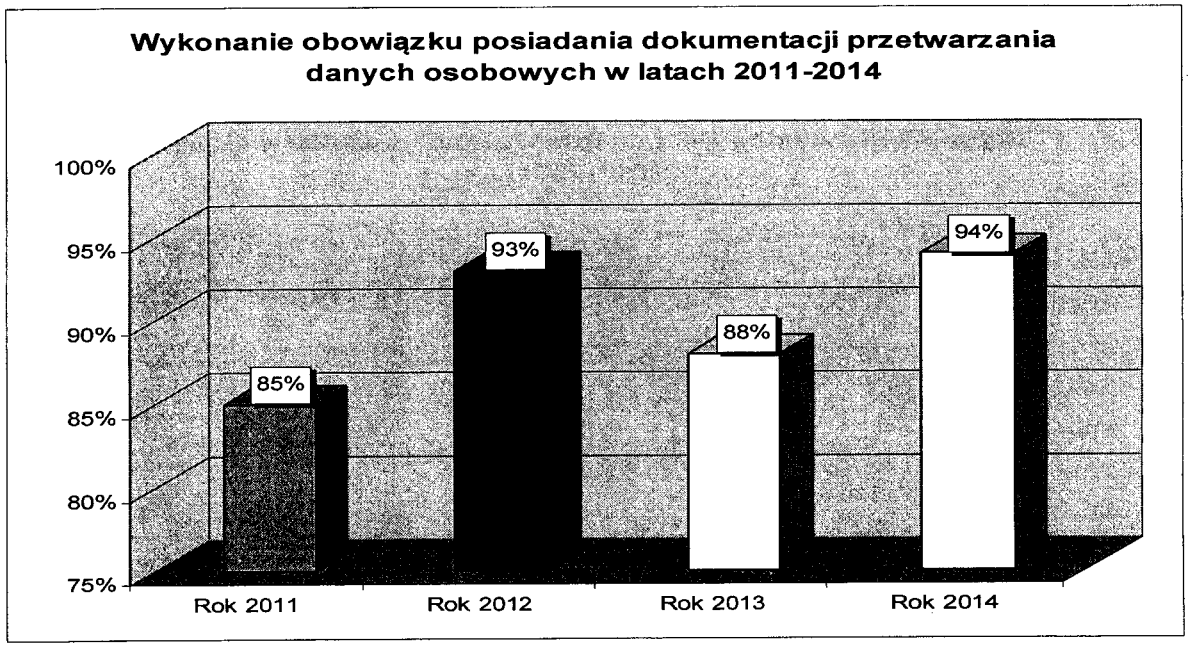
2.4. Wyniki kontroli w zakresie obowiązków formalnych i organizacyjnych.

Spełnienie przez kontrolowane podmioty w latach 2011-2014 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 odnoszące się do prowadzonej

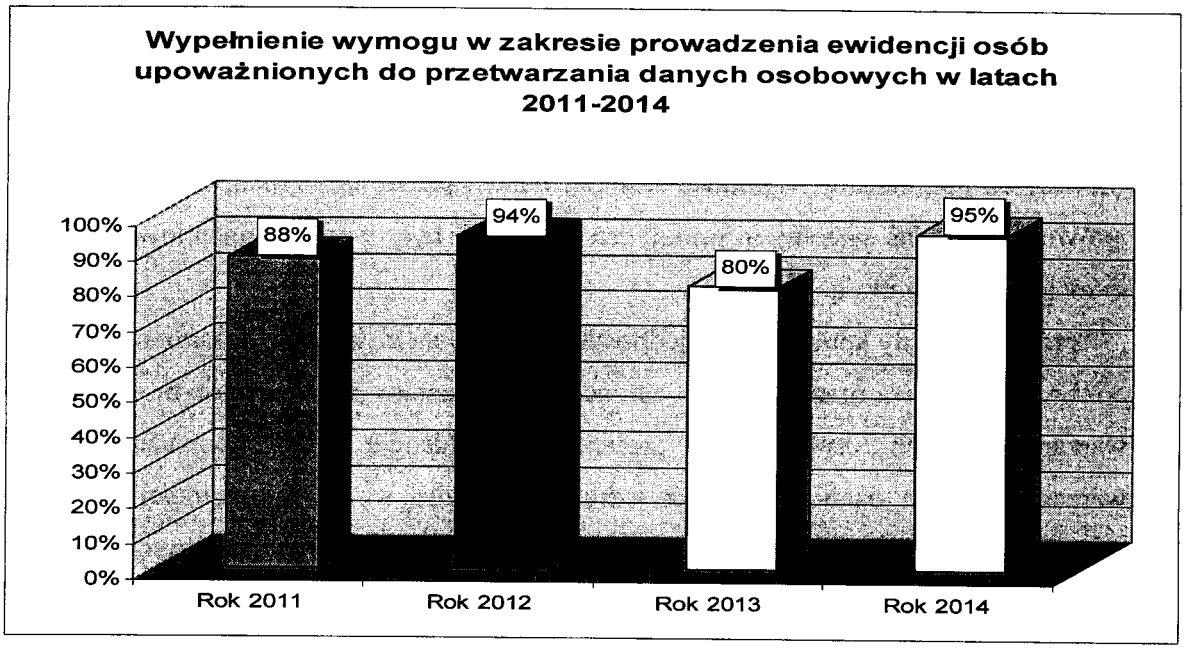
dokumentacji procesu przetwarzania danych, obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, czy też powołania administratora bezpieczeństwa informacji oceniano w skali procentowej w stosunku do liczby kontrolowanych podmiotów. Natomiast warunki odnoszące się do wymagań funkcjonalnych jakie powinny posiadać systemy informatyczne oceniane były w skali procentowej do liczby systemów objętych kontrolą.

W przypadku, gdy kontrolowana jednostka opracowała wymagane dokumenty (takie jak polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych), prowadziła ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wdrożyła opisane w tej dokumentacji procedury 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 2011-2014 przedstawiono na poniższych wykresach.

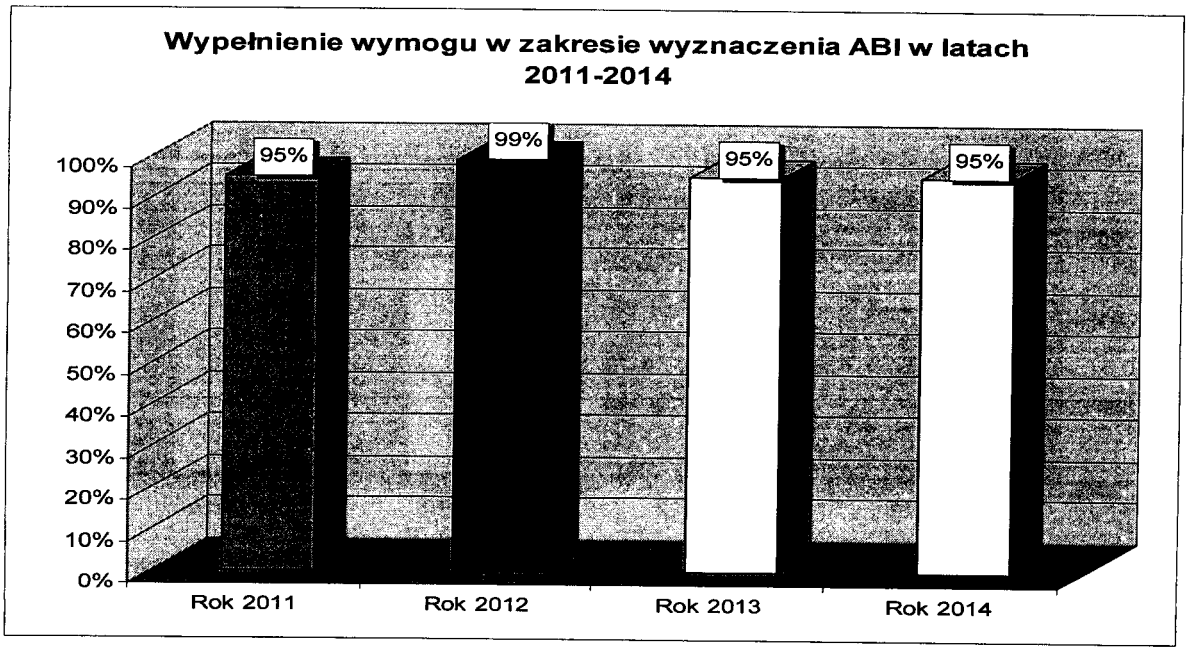


Wykres 3: ***Stopień wykonania obowiązku posiadania dokumentacji przetwarzania danych osobowych (polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym).***



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

Zbiorcze zestawienie wypełnienia wymogów formalnych i organizacyjnych w latach 2011-2014 w zakresie realizacji obowiązku wyznaczenia osoby pełniącej zadania administratora bezpieczeństwa informacji (ABI), przedstawiono na poniższym wykresie.

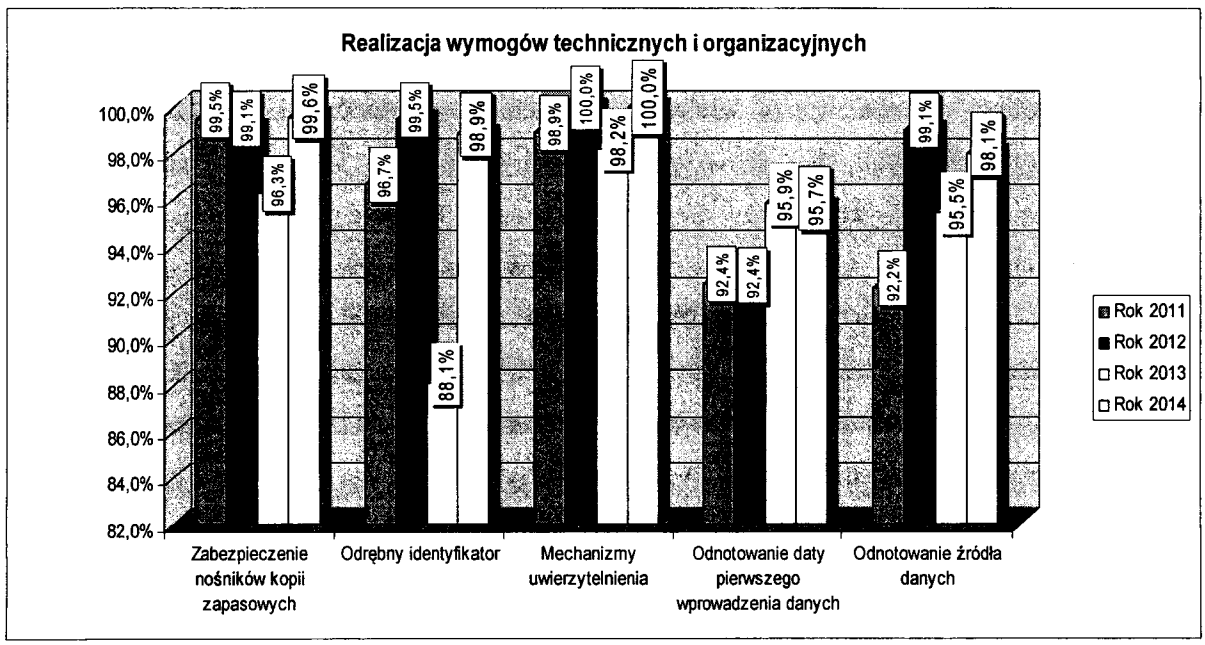


Wykres 5: ***Stopień realizacji obowiązku w zakresie wyznaczenia administratora bezpieczeństwa informacji.***

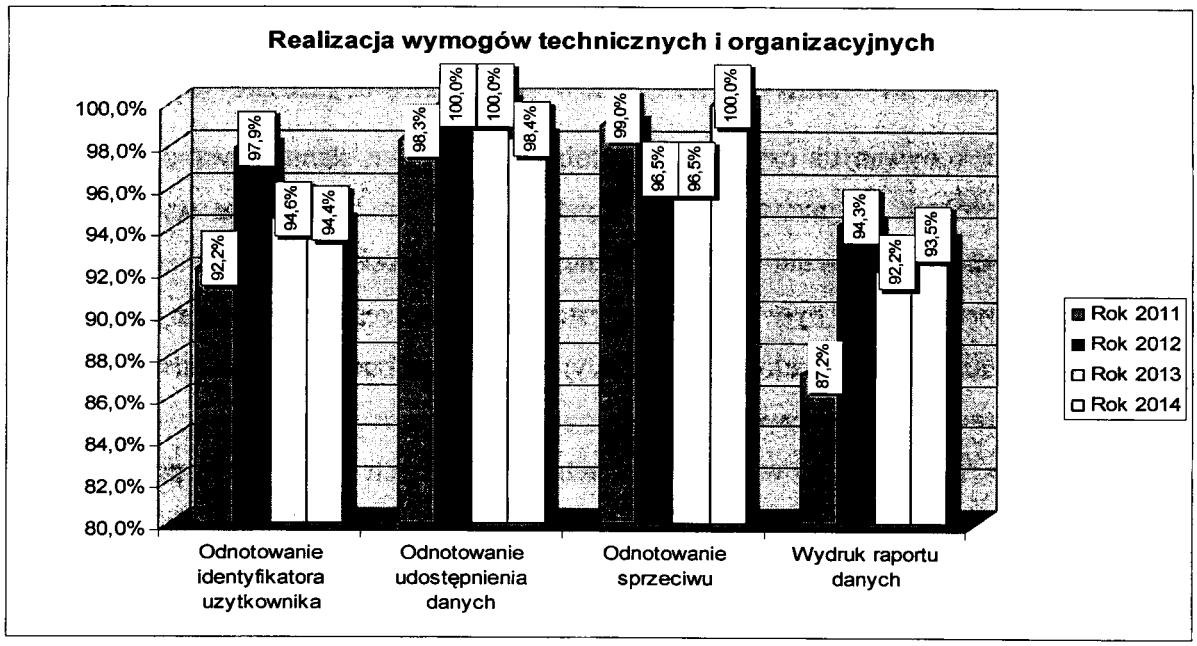
2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych.

Podczas dokonywanych czynności kontrolnych w 2014 r. skontrolowano 362 systemy informatyczne służące do przetwarzania danych osobowych. Systemy te wykorzystywały 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 2014 w porównaniu do lat 2011-2013 przedstawiono na poniższych wykresach.



Wykres 6: ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2011-2014 – część I.***



Wykres 7: ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2011-2014 – część II.***

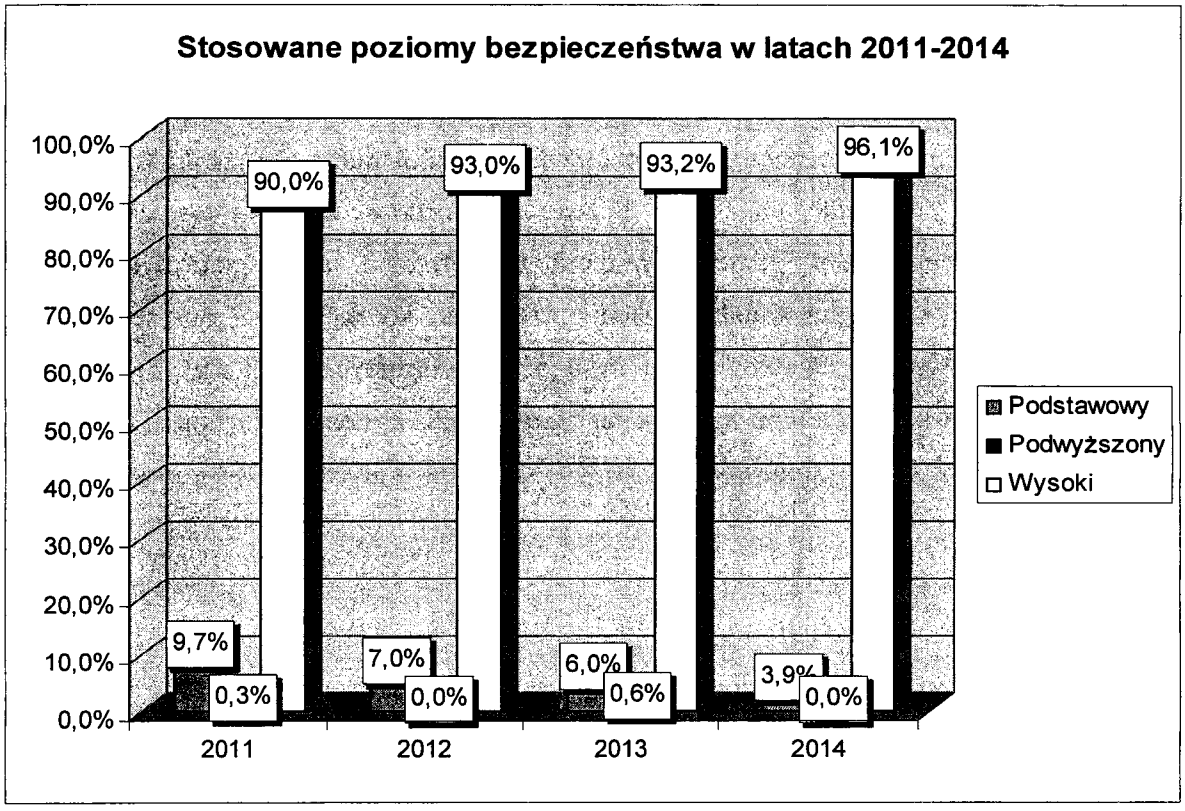
Jak wynika z przedstawionych wykresów, liczba systemów informatycznych objętych kontrolą w roku 2014 była na zbliżonym poziomie do lat 2011-2013. W większości przypadków dane osobowe były przetwarzane w specjalistycznych systemach informatycznych dostosowanych funkcjonalnie do sposobu i zakresu ich przetwarzania. Zauważyć należy również, że w wielu podmiotach do przetwarzania danych osobowych używano zintegrowanych systemów informatycznych, które wykorzystywane były do przetwarzania kilku różnych zbiorów danych osobowych. W systemach tych dane odnoszące się do różnych kategorii spraw przetwarzane były w jednej bazie danych, a ich podział na różne zbiory danych wg klasyfikacji odnoszącej się do celu, czy też zakresu przetwarzania danych, realizowany był logicznie poprzez przypisanie odpowiednich uprawnień i powiązań odnoszących się do struktur informacyjnych dla poszczególnych kategorii danych. Czynnik ten miał istotny wpływ na mniejszą liczbę sprawdzanych systemów informatycznych.

W 2014 roku, w porównaniu z rokiem poprzednim można zaobserwować poprawę realizacji obowiązku dotyczącego konieczności stosowania odrębnych identyfikatorów oraz stosowania mechanizmów uwierzytelniania. Zapewnienie funkcjonalności związanych z odnotowywaniem, przez objęte w 2014 roku kontrolą systemy informatyczne, informacji o dacie oraz identyfikatorze użytkownika wprowadzającego dane, jak również możliwość

sporządzenia raportów z ww. odnotowaniami, kształtuje się na poziomie zbliżonym do lat poprzednich.

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

Podział na poziomy bezpieczeństwa w odniesieniu do skontrolowanych w latach 2011 - 2014 r. systemów informatycznych przedstawiony został na poniższym wykresie.

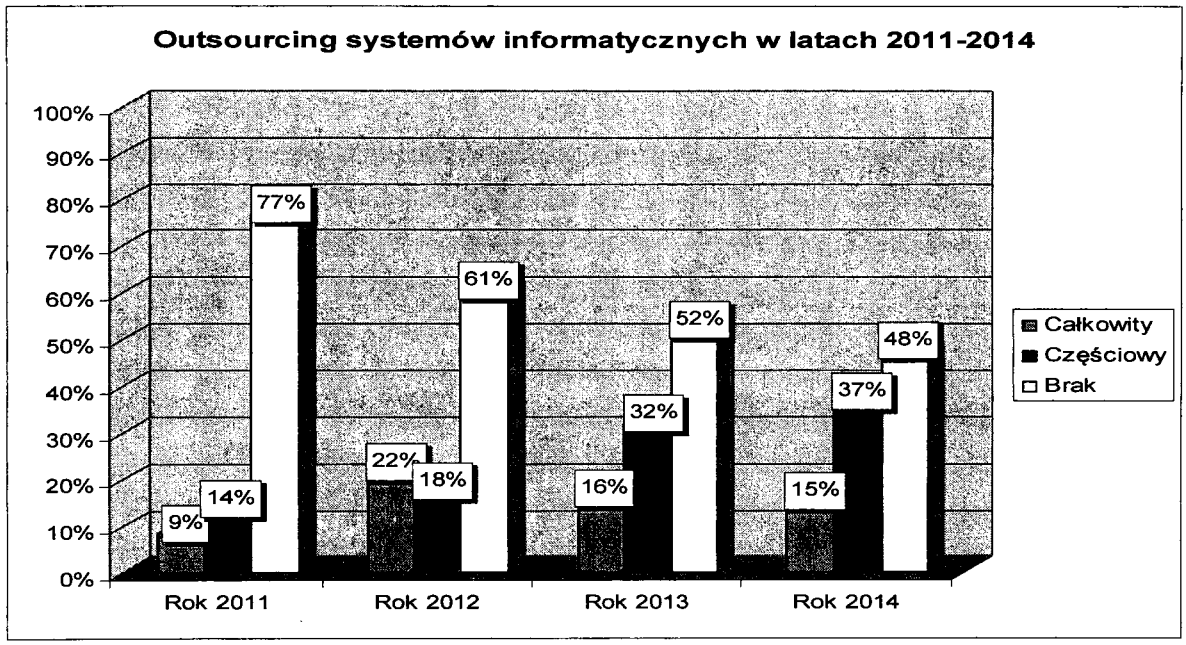


Wykres 8: ***Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w latach 2011-2014.***

Jak wynika z ww. wykresu, większość podmiotów skontrolowanych w 2014 r. (96,1%) zastosowała wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Stwierdzono tym samym proporcjonalny spadek zabezpieczeń na poziomie podstawowym. Wiąże się to z tym, że większość kontrolowanych w 2014 r. podmiotów wykorzystywało systemy informatyczne, które były podłączone do sieci publicznej, a co za tym idzie, wymaganym dla nich poziomem zabezpieczenia był poziom wysoki. W toku

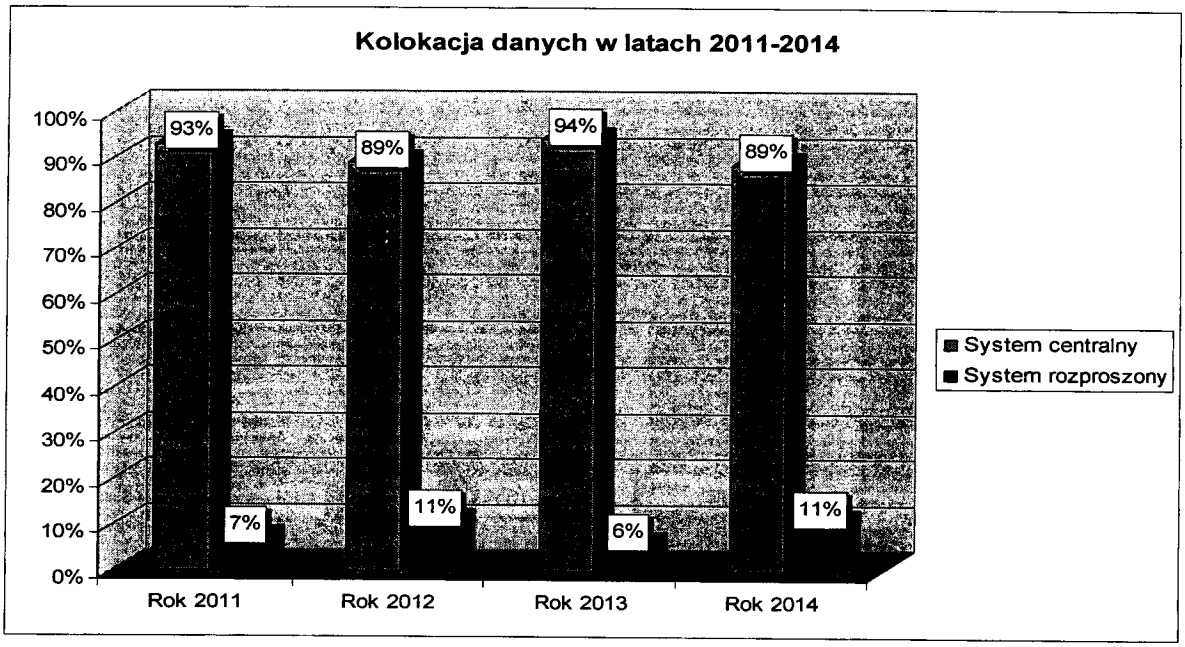
przeprowadzonych w 2014 r. czynności kontrolnych nie stwierdzono przypadków stosowania podwyższonego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, co oznacza, że wszystkie kontrolowane w 2014 r. systemy informatyczne wykorzystywane do przewarzania danych wrażliwych połączone były z siecią publiczną.

Jak wynika z przeprowadzonych w 2014 r. kontroli większość podmiotów wykorzystywało do przetwarzania danych osobowych systemy informatyczne, nad którymi sprawowały pełną kontrolę w zakresie zarządzania i administrowania nimi. Całkowity outsourcing, gdzie proces przetwarzania danych osobowych, jak również oprogramowanie i sprzęt teleinformatyczny administrator danych powierzył w całości do administrowania podmiotom zewnętrznym, w 2014 r. stosowany był w odniesieniu do około 15 % systemów informatycznych. Jest to liczba nieco mniejsza niż w latach ubiegłych. W 2014 r. odnotowano również niewielki spadek liczby tych systemów informatycznych, których obsługą techniczną i administracją zajmowali się wyłącznie pracownicy administratora danych (48% systemów informatycznych). Wzrosła natomiast liczba systemów informatycznych objętych częściowym outsourcingiem, gdzie podmiotom zewnętrznym powierzano tylko niektóre aspekty związane z utrzymywaniem systemu, takie jak 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 37% skontrolowanych w 2014 r. systemach.



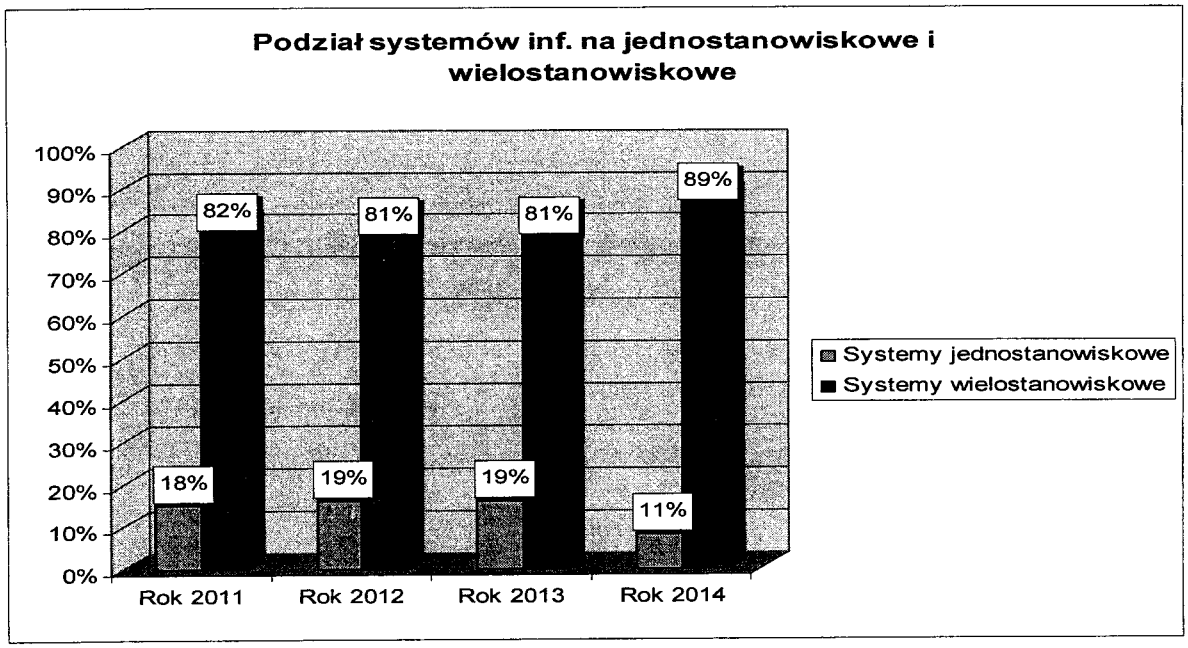
Wykres 9: ***Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2011-2014.***

W 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 stosunku do roku 2013 zwiększyła się liczba podmiotów wykorzystujących do przetwarzania danych osobowych systemy rozproszone. Poniżej przedstawiono diagram ilustrujący stopień stosowania przez kontrolowane podmioty rozwiązań technicznych opartych o systemy centralne i rozproszone.



Wykres 10: ***Ilościowy udział centralnego/rozproszonego przetwarzania danych w systemach informatycznych objętych kontrolą w latach 2011 - 2014.***

Jak przedstawiono na powyższym wykresie w 2014 r. w porównaniu z latami 2011 - 2013 liczba wykorzystywanych wielostanowiskowych systemów informatycznych znajduje się na zbliżonym poziomie (89%). Rozwiązania oparte o systemy jednostanowiskowe stanowiły niecałe 11% skontrolowanych systemów informatycznych. Zastosowanie systemów jednostanowiskowych w większości przypadków dotyczyło przestarzałych rozwiązań informatycznych. Zauważyć jednak należy, że systemy jednostanowiskowe stosowano również w przypadkach, gdy wymagała tego specyfika ich zastosowania (np. systemy monitoringu).



Wykres 11: ***Procentowy udział systemów informatycznych jedno- i wielostanowiskowych wśród systemów objętych kontrolą w latach 2011-2014.***

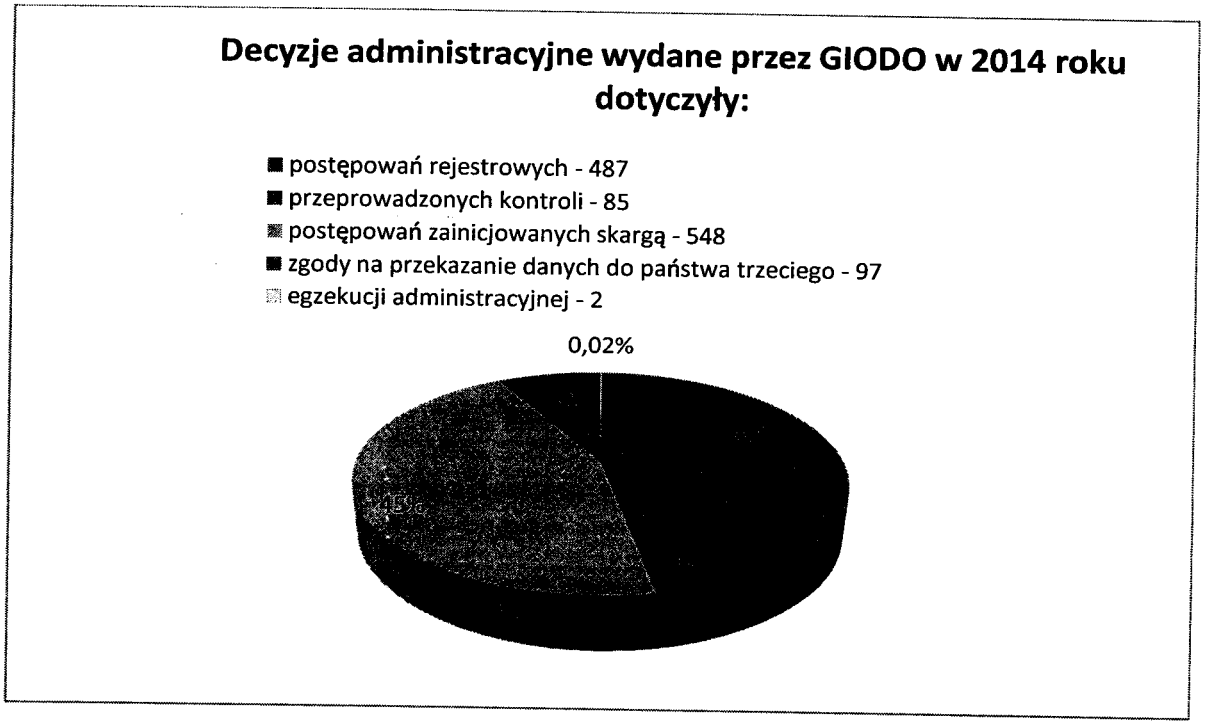
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych.

3.1. Wydawanie decyzji.

Postępowanie dotyczące naruszenia ustawy o ochronie danych osobowych, wszczęte przez Generalnego Inspektora z urzędu lub na wniosek osoby zainteresowanej, prowadzone jest według przepisów ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2013 r. poz. 267 z późn. zm.). 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 2014 r. Generalny Inspektor wydał **1219 decyzji administracyjnych,** tj. o 139 mniej w stosunku do roku 2013, w którym wydanych było 1358 decyzji. Spośród 1219 decyzji wydanych w 2014 r. **487 dotyczyło postępowań rejestrowych, 85 zostało wydanych w**

związku z przeprowadzonymi kontrolami, 548 wydano na skutek postępowania zainicjowanego skargą, zaś 97 dotyczyło zgody na przekazanie danych do państwa trzeciego. Pośród 1219 decyzji, **dwie** z nich dotyczyły **egzekucji administracyjnej**.



Wykres 12: ***Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2014 r.***

3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa.

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych skierował do organów powołanych do ścigania przestępstw **10 zawiadomień o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych**. W porównaniu z rokiem 2013, w którym wystosowano 16 zawiadomień, stanowi to nieznaczny spadek. 7 zawiadomień złożonych zostało w związku z informacjami przekazanymi Generalnemu Inspektorowi Ochrony Danych Osobowych przez podmioty indywidualne, zaś 3 zawiadomienia złożone zostały w wyniku informacji powziętych w trakcie prowadzenia czynności kontrolnych. Należy w tym miejscu zaznaczyć, że na ogólną liczbę 10 zawiadomień skierowanych do organów ścigania, jedno dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w art. 49 ust. 1 ustawy, przetwarzania danych osobowych przez podmioty nieuprawnione poprzez przetwarzanie tych

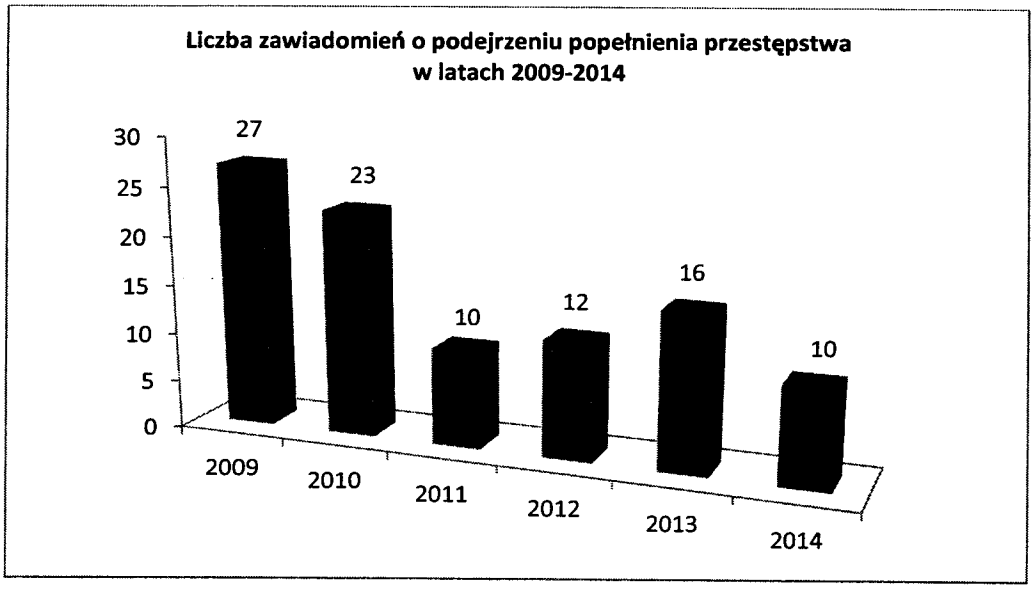
danych bez odstawy prawnej. W toku przeprowadzonego postępowania Generalny Inspektor ustalił, iż wykorzystano dane osobowe skarżącej w celu rzekomego zawarcia umowy i otrzymania od skarżącej zapłaty z tytułu ww. umowy.[79]

Ponadto w 2 przypadkach zawiadomienie dotyczyło przestępstwa wskazanego w art. 51 ustawy, tj. udostępnienia danych osobowych podmiotom nieupoważnionym. W jednej ze spraw do Urzędu Miasta P. wpłynęło skierowane m.in. przez skarżących, zawiadomienie o zamiarze przeprowadzenia referendum gminnego w sprawie odwołania Prezydenta Miasta P.[80] Następnie Wiceprezydent Miasta P. – pracownik Urzędu skierował przeciwko osobom, które podpisały się pod ww. zawiadomieniem wniosek do Sądu w trybie art. 35 ustawy z dnia 15 września 2000 r. o referendum lokalnym. W toku postępowania organ ds. ochrony danych osobowych ustalił, iż ww. urzędnik z racji pełnionej funkcji nie zajmował się kwestiami związanymi z referendum. Wiceprezydent zaprzeczył jakoby otrzymał kopię wniosku skarżących od prezydenta odmawiając jednocześnie wskazania źródła pozyskania ww. danych. Kolejne zawiadomienie dotyczyło umożliwienia przez bank dostępu do informacji o historii rachunku skarżącego na rzecz jego byłej żony.[81]

4 zawiadomienia dotyczyły przestępstw wskazanych zarówno w art. 51 i art. 52 ustawy o ochronie danych osobowych. Generalny Inspektor uzyskał informację o zdarzeniu mającym miejsce w siedzibie spółki, które miałoby polegać na wyrzucaniu przez jej pracowników dokumentów zawierających dane osobowe klientów do kosza na śmieci.[82] Jedno z zawiadomień dotyczyło braku zabezpieczenia danych osobowych zawartych w zestawieniu zamówień realizowanych przez przedsiębiorcę, a w konsekwencji umożliwieniu dostępu do tych danych osobom nieupoważnionych.[83] W kolejnym z zawiadomień podniesiono podejrzenie popełnienia przestępstwa polegającego na braku zabezpieczenia danych osobowych w serwisie internetowym zawierającym dostęp do faktur wystawianych przez spółkę, a dostępnych w internecie.[84] W innej sprawie Generalny Inspektor Ochrony Danych Osobowych pozyskał informację, iż spółka zmieniając siedzibę pozostawiła w poprzednim miejscu dokumentację medyczną osób korzystających z jej usług.[85]

[79] DOLiS/ZAW-9/14/99512.
[80] DOLiS/ZAW-8/14/97172.
[81] DOLiS/ZAW-10/14/101941.
[82] DOLiS/ZAW-3/14/57426.
[83] DOLiS/ZAW-2/14/23692.
[84] DOLiS/ZAW-5/14/64832.
[85] DOLiS/ZAW-7/14/80147.

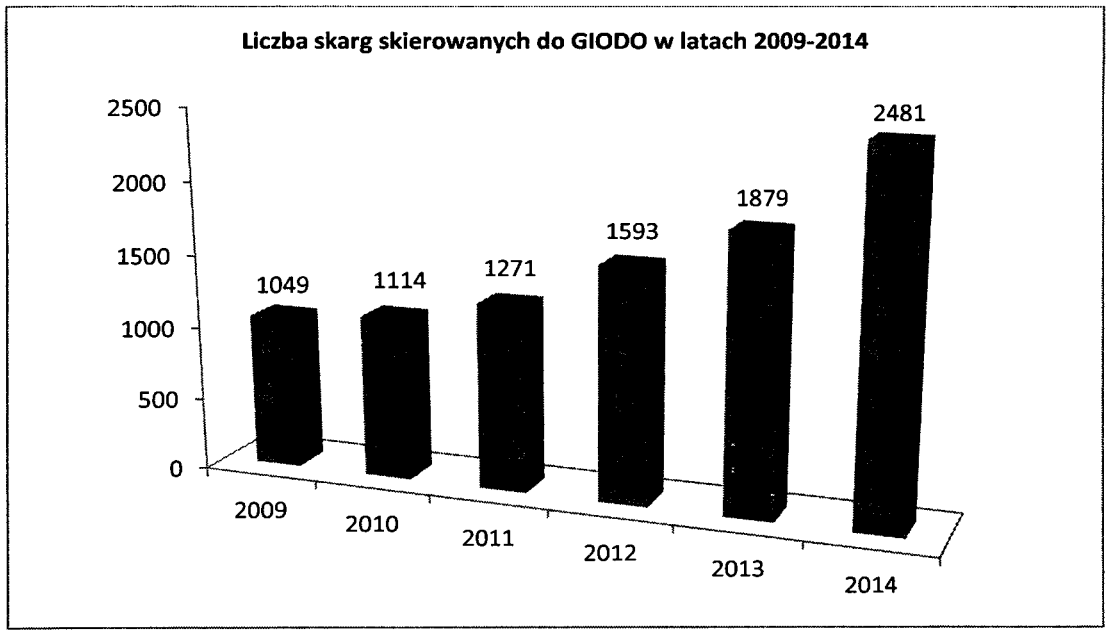
Liczbę zawiadomień o podejrzeniu popełnienia przestępstwa składanych przez Generalnego Inspektora w latach 2009-2014 przedstawia poniższy wykres:



Wykres 13: ***Porównanie liczby zawiadomień o podejrzeniu popełnienia przestępstwa skierowanych przez GIODO do organów ścigania w latach 2009–2014.***

3.3. Rozpatrywanie skarg.

W 2014 r. do Departamentu Orzecznictwa, Legislacji i Skarg wpłynęło **2481** skarg dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2013, w którym wpłynęło 1879 skarg, liczba ta uległa zwiększeniu o 602.



Wykres 14: ***Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2009–2014.***

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. z 2014 r. poz. 1682). W sytuacji, gdy skarga nie spełnienia warunków wymaganych przez ww. przepisy prawa, organ ochrony danych osobowych wzywa wnioskodawcę do uzupełnienia braków formalnych. Skutkiem powyższej analizy **124** skarg z 2014 r. 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.

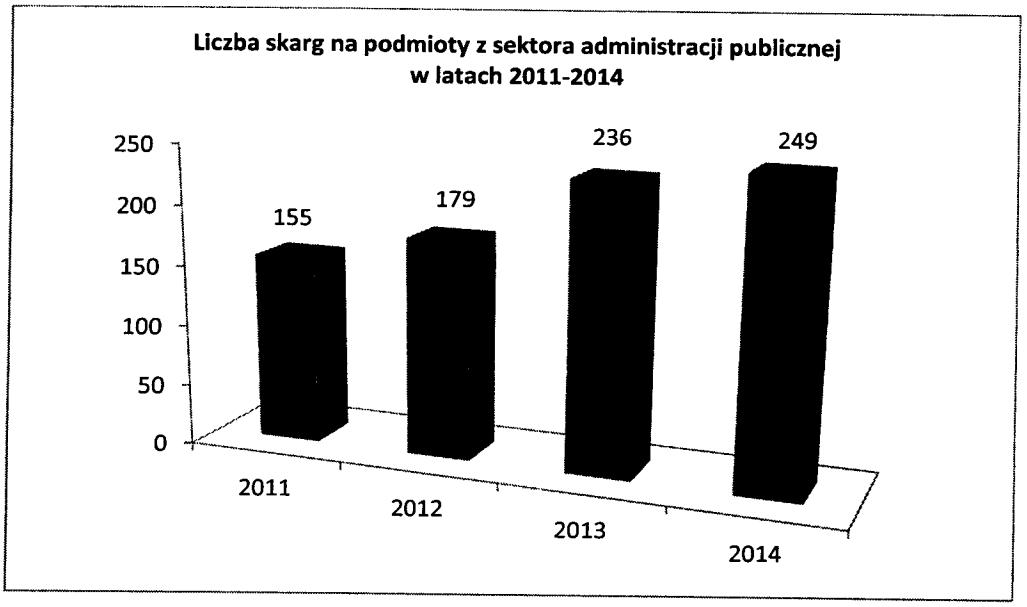
Jeżeli w ich toku stwierdzał naruszenie przepisów ustawy o ochronie danych osobowych, wydawał decyzje administracyjne i zgodnie z art. 18 ustawy o ochronie danych osobowych nakazywał przywrócenie stanu zgodnego z prawem, a w szczególności: 1) usunięcie uchybień, 2) uzupełnienie, uaktualnienie, sprostowanie, 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 **197** sprawach, **133** razy **nakazywał** przywrócenie stanu zgodnego z prawem, zaś w **109** przypadkach **umorzył** postępowanie administracyjne zainicjowane skargą.

Poniżej przedstawione zostały przykłady skarg, które wpłynęły w 2014 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych na podmioty działające w wybranych obszarach.

3.3.1. Administracja publiczna.

W roku 2014 wpłynęło **249 skarg** dotyczących sektora **administracji publicznej**, tj. o 13 więcej niż w roku 2013, w którym wpłynęło 236 skarg z tego zakresu. Wiele skarg dotyczyło braku zanonimizowania dokumentów, takich jak protokoły czy uchwały, zawierających dane osobowe skarżących, i umieszczania ich w takiej formie przez samorządy terytorialne w Biuletynie Informacji Publicznej.



Wykres 15: ***Zestawienie porównawcze liczby skarg na podmioty z sektora administracji publicznej, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2014.***

W omawianym okresie GIODO wydał decyzję odmawiającą uwzględnienia wniosku[86] - w sprawie skargi dotyczącej udostępnienia przez jednego z wojewodów danych osobowych

[86] Decyzja GIODO z 14 lutego 2014 r. (DOLiS/DEC-126/14/11630,11635,11640).

skarżących zawartych w Operacie szacunkowym zamiennym nieruchomości gruntowej na rzecz radcy prawnego. W treści skargi pełnomocnik skarżących podniósł w szczególności, iż przed wojewodą toczyło się postępowanie w przedmiocie ustalenia odszkodowania za nieruchomość, na której prowadzona była działalność gospodarcza. Nieruchomość ta zgodnie z decyzją Wojewody była przeznaczona pod budowę skrzyżowania drogi krajowej z inną drogą. Występujący w innej sprawie odszkodowawczej pełnomocnik radca prawny wystąpił do wojewody o udostępnienie operatu szacunkowego sporządzonego na potrzeby ustalenia odszkodowania, zaś wojewoda operat ten udostępnił. Operat ten został wydany bez zezwolenia stron. Zawierał on takie dane jak nr księgi wieczystej, nr działki, imiona i nazwiska właścicieli. Ponadto urząd wydał radcy prawnemu pisma będące pismami składanymi w toku postępowania odszkodowawczego. W ww. decyzji Generalny Inspektor Ochrony Danych Osobowych stwierdził, iż w przedmiotowej sprawie przy realizacji obowiązku udostępnienia informacji publicznej w postaci kserokopii operatu na rzecz radcy prawnego, w treści których udostępniono imiona i nazwisko skarżących, a także numer księgi wieczystej nieruchomości, której dotyczy przedmiotowy Operat, a której skarżący byli właścicielami, nie uwzględniono ich prawa do prywatności. Jednocześnie została naruszona zasada adekwatności. Zdaniem organu ochrony danych osobowych, przy udostępnieniu operatu jedynie w celu informacyjnym zbędne było (nieadekwatne do celu) ujawnianie imion i nazwisk skarżących oraz numeru księgi wieczystej. Wskazać należy, że udostępnienie dokumentu, który zawiera dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinno nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych. W niniejszej sprawie oznaczało to, że operat powinien zostać udostępniony po uprzednim usunięciu danych osobowych skarżących w zakresie ich imion i nazwiska oraz numeru księgi wieczystej. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych usunięcie samych adresów zamieszkania skarżących z załączników do operatu, stanowiących jego integralną całość, było niewystarczające. Udostępnienie zatem przez wojewodę na rzecz radcy prawnego numeru księgi wieczystej nieruchomości, której skarżący byli właścicielami, prowadziło do sytuacji, w której osoby zapoznające się z treścią udostępnionego dokumentu operatu mogły w sposób niewymagający nadmiernych kosztów, czasu lub działań, zapoznać się z zawartymi w księdze danymi osobowymi skarżących będących byłymi właścicielami ujawnionymi w przedmiotowej księdze wieczystej. Jednocześnie z uwagi na to, iż działanie wojewody było działaniem jednorazowym, proces udostępnienia danych nastąpił i w chwili wydania decyzji nie można było stwierdzić, by stan naruszenia prawa do ochrony danych

osobowych skarżących, kwestionowany w niniejszej sprawie, był przez wojewodę kontynuowany, brak było podstaw do sformułowania pod jego adresem któregokolwiek z nakazów wymienionych w art. 18 ust. 1 ustawy. Jednakże, w celu uniknięcia podobnych uchybień w procesie przetwarzania danych osobowych przez wojewodę, Generalny Inspektor Ochrony Danych Osobowych wystosował do niego wystąpienie[87], w którym zasygnalizował konieczność przestrzegania zasad przetwarzania danych osobowych wynikających z ustawy o ochronie danych osobowych w celu poszanowania prawa do prywatności w trakcie udostępniania informacji publicznej.

W 2014 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga dotycząca udostępnienia danych osobowych skarżącego przez Powiatowego Inspektora Nadzoru Budowlanego dla miasta na prawach powiatu osobom nieupoważnionym[88]. Skarżący w treści skargi wskazał, iż w czerwcu 2012 r. stał się świadkiem „samowoli budowlanej" na działce, której w ocenie skarżącego, dopuściła się Spółka. skarżący zgłosił to do Powiatowego Inspektoratu Nadzoru Budowlanego dla miasta na prawach powiatu. W piśmie skierowanym do ww. organu skarżący zwrócił się z prośbą o nieujawnianie jego tożsamości. PINB wszczął postępowanie, w trakcie którego potwierdził zaistnienie „samowoli budowlanej". Jednocześnie w korespondencji skierowanej do spółki, w toku przedmiotowego postępowania kilkukrotnie zostało wymienione imię i nazwisko skarżącego jako osoby składającej skargę, która je zainicjowała. Pismo skarżącego, pomimo iż nie był on stroną postępowania zostało załączone do akt postępowania prowadzonego przez PINB i udostępnione spółce stosownie do przepisów Kodeksu postępowania administracyjnego, w ramach realizacji przez spółkę prawa do wglądu do akt postępowania. W związku z powyższym, skarżący wniósł o podjęcie przez Generalnego Inspektora Ochrony Danych Osobowych działań mających na celu przywrócenie stanu zgodnego z prawem poprzez zaprzestanie udostępniania jego danych osobowych w ww. sposób. W dniu 28 lutego 2014 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną, mocą której odmówił uwzględnienia wniosku skarżącego[89]. Analiza materiału dowodowego zgromadzonego w przedmiotowej sprawie jednoznacznie wskazała, że pozyskanie danych osobowych skarżącego przez PINB nastąpiło w wyniku zgłoszenia przez skarżącego tzw. „samowoli budowlanej", której był świadkiem. Zdaniem GIODO dalsze udostępnienie danych skarżącego stanowiło już naruszenie przepisów ustawy o

[87] Pismo GIODO z dnia 14 lutego 2014 r. (DOLiS-440-1316/12/11617).
[88] DOLiS-440-71/13.
[89] Decyzja GIODO z dnia 28 lutego 2014 r. (znak: DOLiS/DEC – 181/14/15444,15447).

ochronie danych osobowych. W przedmiotowej sprawie doszło do nieadekwatnego, w stosunku do celu pozyskania, udostępnienia danych osobowych skarżącego. Podkreślenia wymagało, iż skarżący nie stał się stroną postępowania przeprowadzonego przez PINB w sprawie prowadzenia robót budowlanych przez Spółkę bez stosownego pozwolenia organu administracji architektoniczno - budowlanej. Niewątpliwie PINB jako podmiot właściwy do rozpatrywania spraw z zakresu naruszeń przepisów Prawa budowlanego, miał prawo przetwarzać dane osobowe skarżącego, jako osoby zgłaszającej ich naruszenie, jednak w ocenie Generalnego Inspektora, niewłaściwym było ich dalsze udostępnienie podmiotowi, który tego naruszenia się dopuścił. Podkreślenia również wymaga, iż skarżący nie otrzymał statusu strony postępowania prowadzonego przez PINB w sprawie prowadzenia robót budowlanych przez spółkę bez stosownego pozwolenia organu administracji architektoniczno – budowlanej, bowiem nie dotyczyło ono jego interesu prawnego, bądź obowiązku. Dlatego też zawiadomienie skarżącego, wraz z jego danymi, nie powinno było zostać przez PINB włączone do akt ww. postępowania. Biorąc jednakże pod uwagę nieodwracalny charakter udostępnienia danych osobowych skarżącego w ww. formie, w ocenie Generalnego Inspektora właściwym było wydanie decyzji odmawiającej uwzględnienia wniosku. Jednocześnie w ww. dacie Generalny Inspektor Ochrony Danych Osobowych skierował do PINB wystąpienie[90], w którym - w związku z uchybieniami stwierdzonymi w niniejszym postępowaniu polegającymi na udostępnianiu przez PINB danych osobowych osób składających zawiadomienia o naruszeniu przepisów ustawy z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. z 2013 r. poz. 1409 z późn. zm.) przez inne podmioty tymże podmiotom - zwrócił się o zaprzestanie stosowania ww. praktyki jako naruszającej przepisy ustawy o ochronie danych osobowych.

3.3.2. Bezpieczeństwo publiczne.

W analizowanym okresie do GIODO wpłynęło **78 skarg** dotyczących sektora **bezpieczeństwa publicznego**.

Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 28 stycznia 2014 r.[91], wskazał, iż cyt.: „(...) organy Policji są więc uprawnione do przetwarzania danych osób nie tylko podejrzanych o popełnienie przestępstwa, ale także skazanych prawomocnym wyrokiem sądu, jak również tych, wobec których skazanie uległo zatarciu. Realizowanie bowiem celu, jakim jest zapewnienie bezpieczeństwa i porządku publicznego przez organy Policji,

[90] Pismo GIODO z dnia 28 lutego 2014 r. (DOLiS-440-71/13/OS/I/15450/14).
[91] Wyrok WSA w Warszawie z dnia 28 stycznia 2014 r. (sygn. akt II SA/Wa 1366/13).

wykazuje przesłankę niezbędności przetwarzania danych osobowych w Krajowym Systemie Informacyjnym Policji dla spełnienia obowiązku wynikającego z przepisu prawa (art. 1 ust. 2 ww. ustawy o Policji), co oznacza, że sam proces przetwarzania zawartych w tym zbiorze danych ma oparcie w legalnej przesłance przetwarzania danych, o której mowa w art. 23 ust. 1 pkt 2 ww. ustawy o ochronie danych osobowych. Kryterium niezbędności przetwarzania danych osobowych w KSIP musi być odnoszone do ustawowych zadań Policji, których realizowaniu mają służyć przepisy art. 20 ust. 1, ust. 2a i 2b w związku z art. 20 ust. 17 ww. ustawy o Policji. Mechanizm działania zasady proporcjonalności nakazuje, by realizacja tych zadań odbywała się z poszanowaniem generalnych zasad konstytucyjnych, czyli zasady państwa prawnego (art. 2 Konstytucji RP) i zasady legalizmu, wywodzonej z art. 7 ustawy zasadniczej. Wprowadzenie uregulowań ustawowych, które zezwalają organom Policji na przetwarzanie danych osobowych osób wchodzących w konflikt z prawem, mieści się więc w ramach zasady demokratycznego państwa prawnego i zasady legalizmu, wszak zapewnienie ładu i porządku publicznego oraz bezpieczeństwa obywateli jest interesem nadrzędnym Państwa, realizowanym między innymi przez organy Policji. Tym samym niewłaściwe byłoby pozbawienie organów Policji dostępu do jak najpełniejszej informacji, którą Policja sama wytworzyła w sposób legalny."

W związku z powyższym, bazując na rozstrzygnięciu WSA Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił uwzględnienia wniosku[92], z uwagi, iż Komendant Główny Policji przechowywał dane osobowe skarżącego legalnie. Uwzględniając wytyczne sądu administracyjnego GIODO uznał, że to organy Policji oceniają przydatność danych zawartych w KSIP i dokonują ich weryfikacji po zakończeniu sprawy, w ramach której dane te zostały wprowadzone do zbioru, nie rzadziej niż co 10 lat od dnia uzyskania lub pobrania informacji. W rozpoznawanej sprawie okres 10 lat jeszcze nie upłynął. Nadto należy wskazano, że przepis art. 20 ust. 2a ustawy o Policji stanowi *lex specialis* w stosunku do przepisów ustawy o ochronie danych osobowych. Policja może przetwarzać dane osobowe m.in. osób podejrzanych o popełnienie przestępstw nie tylko bez ich zgody, ale co istotne w sprawie bez ich „wiedzy". Jednocześnie wskazano, że KSIP nie stanowi rejestru (zbioru danych osobowych) osób skazanych czy też ukaranych, gdyż takie funkcje pełni Krajowy Rejestr Karny. Informacje, jakimi dysponuje KSIP, nie stanowią źródła wiedzy powszechnie dostępnej, bowiem służą one wyłącznie do realizacji zadań

[92] Decyzja GIODO z dnia 26 sierpnia 2014 r. (znak: DOLiS/DEC-846/14/66449,66452).

Policji, o których mowa w art. 1 ust. 2 ustawy o Policji. Informacje zawarte w KSIP nie mogą służyć jako instrument prawny do prowadzenia polityki kadrowej przez pracodawców.

3.3.3. Sądy, prokuratura, komornicy.

W 2014 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **67 skarg** dotyczących sektora **sądów, prokuratur i komorników**.

GIODO prowadził m.in. postępowanie w sprawie skargi na nieprawidłowości w procesie przetwarzania danych osobowych skarżącego przez prokuraturę rejonową w tym na udostępnienie przez prokuraturę danych osobowych dotyczących jego stanu zdrowia w przygotowawczych postępowaniach karnych, w których nie wydano opinii lub nie złożono zaświadczenia o jego stanie zdrowia. Kwestionowane przez skarżącego działania prokuratury miały za przedmiot jego dane osobowe szczególnie chronione (dane osobowe sensytywne) w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych. Dane osobowe skarżącego to dane objęte aktami prowadzonych przez Prokuraturę postępowań z zawiadomień skarżącego lub przeciwko skarżącemu, w szczególności dane utrwalone w aktach prowadzonych przez prokuraturę postępowań, jak i opinii biegłych. W tym sensie są to więc dane osobowe dotyczące „stanu zdrowia" oraz „innych orzeczeń wydanych w postępowaniu sądowym" w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych. Dane te zostały następnie włączone w celach dowodowych w poczet akt postępowania prowadzonego przez prokuraturę zachowując omawiany status. Generalny Inspektor Ochrony Danych Osobowych odmówił uwzględnienia wniosku[93] skarżącego wskazując, iż kwestionowane działania prokuratury, mające za przedmiot dane osobowe skarżącego, znajdowały oparcie w art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych. W świetle przepisów Kodeksu karnego prokuratura była uprawniona – w sytuacji, gdy zostało to uznane za istotne ze względów dowodowych – do pozyskania z prowadzonych przez siebie wcześniej postępowań kwestionowanych danych osobowych skarżącego.

W 2014 r. Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej odmówił uwzględnienia wniosku[94] skarżącego w sprawie dotyczącej nieprawidłowości w procesie przetwarzania jego danych osobowych przez sąd rejonowy, a

[93] Decyzja GIODO z dnia 9 września 2014 r. (DOLiS/DEC-881/14/70361,70362).
[94] Decyzja GIODO z dnia 3 marca 2014 r. (DOLiS/DEC-183/14/15773,15777).

następnie utrzymał w mocy tę decyzję[95]. Skarżący postawił zarzut, jakoby toczące się w jego sprawie postępowanie o pomówienie było prowadzone przez sąd jako jawne, co stanowi naruszenie art. 359 Kodeksu postępowania karnego. Według twierdzeń skarżącego, przewodniczący, wbrew ciążącej na nim powinności wynikającej z art. 362 K.p.k., nie pouczył obecnych na sali rozpraw o obowiązku zachowania w tajemnicy okoliczności ujawnionych na rozprawie toczącej się z wyłączeniem jawności i nie uprzedził o skutkach niedopełnienia takiego obowiązku. Zgromadzony w sprawie materiał dowodowy nie pozwolił na stwierdzenie, jakoby postępowanie było prowadzone przez sąd jako jawne, w konsekwencji czego nie doszło do przetwarzania danych skarżącego z naruszeniem przepisów ustawy o ochronie danych osobowych. Wobec ustalenia w sprawie, że sąd nie dopuścił się nieprawidłowości w procesie przetwarzania danych osobowych skarżącego brak było podstaw do wydania przez Generalnego Inspektora w stosunku do skarżonego podmiotu jakiegokolwiek nakazu na podstawie ww. art. 18 ust. 1. Ponadto skarżący kwestionował niewywiązanie się przez sędziego sądu z obowiązku pouczenia uczestników rozprawy o obowiązku zachowania w tajemnicy okoliczności ujawnionych na rozprawie toczącej się z wyłączeniem jawności i uprzedzenia o skutkach niedopełnienia tego obowiązku (do czego obliguje przewodniczącego art. 362 K.p.k.), a więc obowiązku nałożonego na niego procedurą karną, czego Generalny Inspektor Ochrony Danych Osobowych nie mógł ocenić albowiem nie może wkraczać w kompetencje zastrzeżone zgodnie z obowiązującymi przepisami prawa dla innych podmiotów.

Inną ze skarg, była skarga komornika sądowego na urząd skarbowy dotycząca kierowania do skarżącego jako komornika sądowego na jego prywatny adres korespondencji służbowej dotyczącej prowadzonych przez niego postępowań komorniczych. Po przeprowadzeniu postępowania administracyjnego w sprawie Generalny Inspektor Ochrony Danych Osobowych decyzją administracyjną nakazał urzędowi sprostowanie danych osobowych komornika przetwarzanych w związku z prowadzonymi przez ww. postępowaniami egzekucyjnymi, w zakresie adresu do korespondencji prowadzonej przez niego kancelarii komorniczej[96]. Organ w ww. decyzji wskazał, iż zbieranie danych osobowych powinno być dokonywane dla celów oznaczonych, nie jest więc dozwolone ich dalsze przetwarzanie niezgodnie z tymi celami. Dotyczy to także przypadków, gdy owo dalsze przetwarzanie dokonywane jest przez tego samego administratora. Wspomniany cel

[95] Decyzja GIODO z dnia 17 lipca 2014 r. (DOLiS/DEC-681/14/55583,55584).
[96] Decyzja GIODO z dnia 27 czerwca 2014 r. (DOLiS/DEC-606/14/48999,49000).

wyznacza zakres przetwarzania danych. W powyższym przypadku pozyskanie prywatnego adresu skarżącego z systemu POLTAX, w którym zdefiniowany jest jako podatnik, a nie jako komornik, wykracza poza cel powyższego systemu. Został więc nałożony w ustawie na administratora danych obowiązek zapewnienia, aby znajdujące się w jego dyspozycji dane nie były poddawane dalszemu przetwarzaniu niezgodnie z celem, dla którego zostały zebrane. W tym przypadku sam administrator dopuścił się złamania tego obowiązku i w świetle powyższego zasadne było sformułowanie ww. nakazu.

3.3.4. Organizacje społeczne.

W roku sprawozdawczym 2014 wpłynęło do Biura GIODO **29 skarg** dotyczących **organizacji społecznych** (oznacza to spadek w stosunku do roku ubiegłego, gdzie liczba tych skarg wyniosła 63).

Jednocześnie w tym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych decyzją[97] m.in. nakazał jednej z fundacji usunięcie ze swojej strony internetowej danych osobowych skarżącego w zakresie jego imienia, nazwiska, daty urodzenia, pseudonimu, imion i nazwisk rodziców, informacji o wykształceniu, miejscach zamieszkania i miejscach pracy. Skarga dotyczyła udostępnienia na stronie internetowej fundacji. zawartości teczki znajdującej się w oddziale Instytutu Pamięci Narodowej, w której znajdowały się też dane skarżącego.

Instytut Pamięci Narodowej wskazał, iż teczka personalna i teczka pracy tajnego współpracownika [ich elektroniczne kopie opublikowano na stronie internetowej fundacji] zostały udostępnione dwukrotnie w celu publikacji materiału prasowego na podstawie art. 36 ust. 1 pkt 3 ustawy o Instytucie Pamięci. Postępowanie wobec IPN zostało umorzone albowiem z dostępnej w Instytucie Pamięci dokumentacji nie wynikało, aby dane osobowe skarżącego zostały udostępnione fundacji. Jednocześnie ze statutu fundacji wynikało, iż celami fundacji są w szczególności działania na rzecz upamiętniania idei i dokonań „Solidarności" z lat 1980-1989 oraz wspierania NSZZ „Solidarność", prowadzenia na rzecz rozwoju społeczeństwa obywatelskiego, popularyzacja wiedzy na temat historii, tworzenie płaszczyzn wymiany informacji i doświadczeń pomiędzy osobami i instytucjami zainteresowanymi tematyką historii i inicjatyw lokalnych, popularyzacja tradycji narodowych, pielęgnowanie polskości oraz rozwój świadomości narodowej, obywatelskiej i kulturowej. W świetle powyższego organ do spraw ochrony danych osobowych nie mógł

[97] Decyzja GIODO z dnia 8 maja 2014 r. (DOLiS/DEC-437/14/35117,35122,35124).

stwierdzić by dane skarżącego fundacja pozyskała w sposób legalny. W szczególności GIODO nie mógł zgodzić się z argumentacją fundacji, iż przedmiotowe udostępnienie danych skarżącego jest wykonywane w celu realizacji zadań statutowych fundacji dla propagowania wśród społeczeństwa wiedzy na temat historii Polski. W ocenie organu dla realizacji statutowych zadań fundacji polegających w szczególności na prowadzeniu działań edukacyjnych na rzecz rozwoju społeczeństwa obywatelskiego i popularyzacji wiedzy na temat historii, które zdaniem fundacji wymagają ujawnienia dokumentów historycznych wyjaśniających najnowszą historię, w tym wypadku z terenu dawnego województwa, nie było niezbędne ujawnienie danych osobowych skarżącego, pozwalających na jego jednoznaczną identyfikację, w zakresie jego imienia, nazwiska, daty i miejsca urodzenia, imion rodziców, informacji o wykonywanym przez skarżącego zawodzie, wykształceniu, miejscach zatrudnienia, miejscach zamieszkania. Dane te, w ocenie organu, powinny były zostać zanonimizowane. Niezależnie od faktu, iż jak twierdziła fundacja, iż pozyskała dane od anonimowej osoby, fundacja, jako administrator danych osobowych, stała się bowiem odrębnym administratorem danych osobowych odpowiedzialnym za dalsze ujawnianie kwestionowanych danych osobowych.

3.3.5. Banki i inne instytucje finansowe.

W omawianym roku sprawozdawczym wpłynęły **354 skargi**, w których zakwestionowano legalność działań **banków i innych instytucji finansowych**, (dla porównania w roku 2013 było ich 247).

W treści jednej z nich skarżąca wskazała, iż po otrzymaniu i sprawdzeniu danych na nowej karcie płatniczej wydanej do jej konta osobistego, zwróciła się dwukrotnie do banku o poprawienie błędu w jej nazwisku. Bank odmówił jej tłumacząc, iż w regulaminie konta zastrzegł sobie możliwość umieszczenia na karcie danych osobowych bez wykorzystania polskich znaków. W toku przeprowadzonego postępowania organ ustalił, iż nazwisko skarżącej przetwarzane przez bank jest merytorycznie niepoprawne. Skutkiem tego nieprawidłowego przetwarzania było figurowanie nazwiska skarżącej na karcie płatniczej banku w formie nieprawidłowej, choć w zbiorze danych przetwarzane były poprawnie. W związku z tym, skarżąca, korzystając z uprawnień określonych w art. 32 ust. 1 pkt 6 ustawy o ochronie danych osobowych, zwróciła się do banku o stosowanie poprawnej pisowni jej nazwiska figurującego m.in. na karcie płatniczej. Z chwilą wystąpienia z tym żądaniem po stronie banku powstał wynikający z ww. przepisów obowiązek sprostowania nazwiska

skarżącej. Tymczasem bank, nie dochowując należytej staranności w zakresie ochrony interesów skarżącej, odmówił sprostowania jej nazwiska. Nadmienić również należy, iż postanowienia regulaminu nie mogą być sprzeczne z powszechnie obowiązującym prawem, stąd nawet jeśli bank zastrzegł sobie w regulaminie, w przypadku kart płatniczych, prawo do przetwarzania danych swoich klientów bez polskich znaków, to nie może odgórnie narzucać klientowi takiego rozwiązania. Klient powinien mieć prawo nie wyrażenia zgody na takie rozwiązanie, bądź też jak w przypadku skarżącej ma prawo żądania sprostowania swoich danych osobowych. Podkreślić przy tym należy, że administrator danych osobowych miał obowiązek stosowania takich rozwiązań technicznych, które pozwolą na przetwarzanie danych osobowych merytorycznie poprawnych. Zatem istniejącego stanu rzeczy nie usprawiedliwiał fakt, iż w obecnie stosowanym przez bank systemie informatycznym nie było możliwości stosowania obcych znaków diakrytycznych. W związku z powyższym niezbędne było wydanie przez Generalnego Inspektora wobec banku nakazu sprostowania nazwiska skarżącej[98].

W 2014 r. GIODO wydał decyzję w sprawie skargi na przetwarzanie danych osobowych przez bank, w tym ich udostępnienia na rzecz Biura Informacji Kredytowej S.A. (BIK) Pełnomocnik skarżącej podniósł, iż żądaniem skarżącej jest zobowiązanie banku do zaprzestania przetwarzania danych osobowych skarżącej w zakresie nieobowiązującej już umowy o kartę kredytową. Z materiału dowodowego zebranego w sprawie wynika, że bank nie dopełnił wobec skarżącej obowiązku informacyjnego wynikającego z przepisu art. 105a ust. 3 Prawa bankowego. Co prawda bank oświadczył, iż pismo informujące skarżącą o zamiarze przetwarzana danych osobowych na podstawie ww. podstawy prawnej było wysyłane do skarżącej, jednakże w aktach sprawy brak było jakiegokolwiek dowodu potwierdzającego fakt otrzymania tego pisma przez skarżącą. Z kolei skarżąca kategorycznie zaprzeczyła jakoby otrzymała ww. oświadczenie banku. W związku z powyższym stwierdzić należało, iż aktualnie brak było podstaw prawnych do przetwarzania przez bank danych osobowych skarżącej w BIK na podstawie art. 105a ust. 3 Prawa bankowego, wynikających z umowy o kartę kredytową. Wobec tego konieczne stało się skorzystanie przez Generalnego Inspektora Ochrony Danych Osobowych z instrumentów prawnych przyznanych mu art. 18 ust. 1 pkt 1 ustawy, i nakazanie bankowi zaprzestania przetwarzania danych osobowych skarżącej w zbiorze danych osobowych prowadzonym przez BIK, przetwarzanych na

[98] Decyzja GIODO z dnia 31 lipca 2014 r. (DOLiS/DEC-755/14/59469,59474).

podstawie art. 105a ust. 3 w zw. z art. 105 ust. 4 Prawa bankowego w związku z umową o kartę kredytową[99].

Wśród wyroków sądów administracyjnych, które zapadły w sprawach związanych z działalnością banków i instytucji finansowych wskazać należy, iż sądy administracyjne wskazują na zasadność stanowiska organu ds. ochrony danych osobowych w tym zakresie. W wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie[100] oddalającego skargę w przedmiocie przetwarzania danych osobowych skarżącego przez bank, BIK oraz ZBP, wskazano, iż cyt.: „Nie ulega wątpliwości, że zarówno BIK należy do instytucji wymienionych w art. 105 ust. 4, a celem przetwarzania danych zawartych w BIK, jak i Związek Banków Polskich (ZBP) jest zwiększenie bezpieczeństwa systemu bankowego i płatniczego oraz ochrona depozytów bankowych oraz ocena zdolności kredytowej i analiza ryzyka kredytowego. Zatem w ocenie Sądu organ prawidłowo ocenił, że do przetwarzania danych na podstawie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych w zw. z art. 105 ust. 4 i 105a ust. 1 ustawy Prawo bankowe - zgoda osoby, której dane są przetwarzane, nie jest wymagana. Powołane przepisy prawa nie ustanawiają bowiem takiego wymogu. O zgodzie na przetwarzanie danych stanowiących tajemnicę bankową przez instytucje wymienione w art. 105 ust. 4 ustawy mowa dopiero w art. 105a ust. 2, tj. po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów. Tymczasem w rozpoznawanej sprawie zobowiązanie wynikające z umowy zawartej z bankiem nie wygasło".

3.3.6. Internet.

W 2014 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **406 skarg** dotyczących **przetwarzania danych osobowych w Internecie**, co stanowiło wzrost liczby skarg o 182 w porównaniu do zeszłego roku. Skargi głównie dotyczyły nieuprawnionego udostępniania danych na różnych portalach internetowych, co w konsekwencji prowadziło do naruszenia praw podmiotów danych.

Generalny Inspektor Ochrony Danych Osobowych prowadził m.in. postępowanie administracyjne w sprawie skargi na odmowę usunięcia danych osobowych skarżącej w postaci jej wizerunku zamieszczonego na stronie internetowej przez przedsiębiorcę. W uzasadnieniu skargi skarżąca wskazała, że w 2006 r. nieodpłatnie i bez żadnej umowy pisała

[99] Decyzja GIODO z dnia 22 października 2014 r. (DOLiS/DEC-1010/14/82451,82455).
[100] Wyrok WSA w Warszawie z dnia 19 lutego 2014 r. (sygn. akt II SA/Wa 1945/13).

artykuły do serwisu internetowego, który w tamtym czasie był serwisem poświęconym modzie, a nie sklepem internetowym. Redaktor naczelny serwisu, po wygranym przez skarżącą konkursie na redaktora, zaproponował jej pisanie artykułów na zasadzie wolontariatu. Jej pierwszy artykuł został opatrzony jej zdjęciem z CV, które zostało wykorzystane bez jej zgody. Jak podaje skarżąca, nie wyraziła również zgody na dysponowanie tym zdjęciem na czas nieokreślony. Po kilku miesiącach skarżąca zakończyła współpracę z serwisem internetowym, ale jej zdjęcie nie zostało usunięte. Po wpisaniu jej danych osobowych (imienia i nazwiska) w wyszukiwarce internetowej, pojawiało się ono w grafikach Google, przekierowując na artykuł z 2006 r. i sklep internetowy oferujący odzież i dodatki, na który w 2009 r. zamieniono w serwis internetowy. Jak poinformowała skarżąca, ze względu na to, że został zmieniony profil działalności, z serwisu z informacjami o modzie na sklep internetowy, nie wyraziła życzenia promocji swoim nazwiskiem tej działalności. skarżąca bezskutecznie kilkakrotnie prosiła właściciela domeny o usuniecie jej zdjęcia. W ocenie Generalnego Inspektora Ochrony Danych Osobowych, przedsiębiorca nie wykazał się żadną z przesłanek legalności przetwarzania danych skarżącej na stronie internetowej w zakresie jej wizerunku, a przede wszystkim nie posiadał zgody skarżącej na publikację jej wizerunku. Nie wykazał także spełnienia innych przesłanek, na mocy których publikacja wizerunku skarżącej byłaby dla przedsiębiorcy niezbędna dla zrealizowania jakiegoś uprawnienia lub spełnienia określonego obowiązku. W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych w drodze decyzji administracyjnej[101] nakazał przedsiębiorcy wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącej w zakresie jej wizerunku poprzez usunięcie go ze strony internetowej.

Wśród wyroków, które zapadły w wyniku skargi podmiotów na decyzje organu ds. ochrony danych osobowych należy w szczególności wskazać na wyroki WSA[102] wskazujące na zasadność dotychczasowego stanowiska GIODO w sprawie udostępniania danych osobowych niezbędnych do dochodzenia praw przed sądem, w szczególności w zakresie numerów IP komputerów, użytkowników forów internetowych. W ww. wyrokach sąd ocenił, iż organ prawidłowo przyjął, że przepis art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, umożliwia udostępnianie danych w ww. celach. W sytuacji bowiem, gdy wnioskodawca zamierza na drodze postępowania cywilnego dochodzić ochrony swoich dóbr

[101] Decyzja GIODO z dnia 8 sierpnia 2014 r. (DOLiS/DEC-791/14/61869,61884).
[102] Wyrok WSA w Warszawie z dnia 18 lipca2014 r. (sygn. akt II SA/Wa 569/14), Wyrok WSA w Warszawie z dnia 18 lipca2014 r. (sygn. akt II SA/Wa 570/14).

osobistych, istnieją podstawy do przyjęcia, że dane osobowe osób znieważających wnioskodawcę, są mu niezbędne dla realizacji »prawnie usprawiedliwionych celów.

3.3.7. Marketing.

W analizowanym okresie do GIODO wpłynęły **153 skargi** na podmioty działające w sektorze **marketingu** (dla porównania w 2013 r. wpłynęły 93 skargi dotyczące tego zakresu). Większość skarg kierowanych do organu ochrony danych osobowych dotyczyła przetwarzania danych osobowych w celach marketingowych pomimo złożonych przez osoby, których dane dotyczą, sprzeciwu wobec takiego działania.

Jedna z takich skarg dotyczyła przetwarzania danych osobowych skarżącego przez bank, w tym na ich udostępnienie na rzecz podmiotów nieupoważnionych. Skarżący wskazał, iż pomimo poinformowania banku o braku zgody na przetwarzanie jego danych osobowych w celach marketingowych, otrzymał on telefon od firmy, której bank powierzył przetwarzanie danych swoich klientów w celu badania satysfakcji z produktów bankowych u swoich klientów. W złożonych wyjaśnieniach bank wykazał, iż był uprawniony do przetwarzania danych osobowych skarżącego z uwagi na dyspozycję art. 23 ust. 1 pkt 3 ustawy, tj. z uwagi na łączącą bank i skarżącego umowę. Bank przetwarzał jego dane w celach niezbędnych do świadczenia usług bankowych. Jednakże wyjaśnienia banku wskazywały, iż po dacie złożenia przez skarżącego sprzeciwu, przetwarzanie danych osobowych skarżącego zostało powierzone w celu zbadania satysfakcji ze świadczonych usług. Generalny Inspektor uznał, - że kwestionowana przez skarżącego działalność tego podmiotu niewątpliwie miała charakter marketingowy. Podmiotem odpowiedzialnym nie była Spółka ale bank jako administrator danych skarżącego. W związku ze zgłoszonym sprzeciwem skarżącego cel w zakresie marketingu w ogóle nie powinien być realizowany przez bank, a tym bardziej dane osobowe skarżącego nie powinny być powierzone Spółce dla realizacji kwestionowanego celu. W związku z powyższym Generalny Inspektor nakazał zaprzestania przetwarzania danych osobowych skarżącego w celach marketingowych[103].

Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie w sprawie skargi dotyczącej zbadania legalności procesu przetwarzania danych osobowych skarżącego przez jednego z operatorów telekomunikacyjnych w związku ze skierowaniem do niego telefonicznie oferty objęcia ochroną ubezpieczeniową przez jedno z towarzystw ubezpieczeniowych. W ocenie Generalnego Inspektora w ten sposób operator

[103] Decyzja GIODO z dnia 30 grudnia 2014 r. (DOLiS/DEC-1214/14/102819,102828).

telekomunikacyjny prowadził marketing produktów i usług podmiotu trzeciego, świadczącego usługi ubezpieczeniowe. Wskazywany przez spółkę argument, iż celem takiej oferty jest jedynie promocja własnych produktów i usług nie został uznany za zasadny. Przedmiotowe działania marketingowe prowadzone były w jego interesie jedynie z racji potencjalnych korzyści finansowych operatora wynikających z zawartej z towarzystwem umowy. Dodatkowo nie bez znaczenia pozostawał fakt, że w przypadku objęcia abonenta operatora telekomunikacyjnego ochroną ubezpieczeniową jego dane osobowe były przekazywane na rzecz towarzystwa ubezpieczeniowego, które stosownie do porozumienia stawało się nowym administratorem danych osobowych. W przedmiotowej sprawie operator telekomunikacyjny, w myśl przyjętych rozwiązań, nie ponosił żadnych kosztów prowadzenia akcji telemarketingowej, a rola operatora sprowadzała się *de facto* do udostępnienia danych osobowych własnych abonentów w związku z tą akcją. Tym samym organ stwierdził, że w przedmiotowej sprawie przedstawiony został produkt ubezpieczeniowy podmiotu trzeciego, czyli towarzystwa ubezpieczeniowego, na rzecz którego działała spółka celowa, której operator telekomunikacyjny powierzył w tym celu przetwarzanie danych osobowych. W związku z powyższym, organ ds. ochrony danych osobowych mocą decyzji administracyjnej[104] nakazał operatorowi telekomunikacyjnemu przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osobowych skarżącego poprzez zaprzestanie przetwarzania jego danych osobowych w celu marketingu produktów i usług towarzystwa ubezpieczeniowego.

3.3.8. Mieszkalnictwo.

W 2014 roku do Biura GIODO wpłynęły **104 skargi** dotyczące zagadnień związanych z **mieszkalnictwem,** co stanowi nieznaczny wzrost w stosunku do poprzedniego roku (dla porównania w roku 2013 r. wpłynęło 93 skargi dotyczące tego sektora). W grupie tych zagadnień przede wszystkim znajdowały się skargi dotyczące przetwarzania danych osobowych skarżących przez spółdzielnie mieszkaniowe i wspólnoty mieszkaniowe.

W analizowanym okresie sprawozdawczym Generalny Inspektor prowadził postępowanie wyjaśniające w sprawie skargi na udostępnienie danych osobowych skarżącego przez prezesa zarządu spółdzielni mieszkaniowej podczas obrad Walnego Zgromadzenia Spółdzielni na rzecz osób nieupoważnionych. W treści ww. skargi skarżący podniósł w szczególności iż w trakcie Walnego Zgromadzenia Spółdzielni jeden z członków dokonał

[104] Decyzja GIODO z dnia 7 listopada 2014 r. (DOLiS/DEC-1078/14/87943,87947).

zgłoszenia skarżącego jako kandydata na członka Rady Nadzorczej. Po przedstawieniu kandydatów Prezes Zarządu Spółdzielni poinformował członków Walnego Zgromadzenia o tym, że dwóch kandydatów pozostaje w sporze sądowym ze Spółdzielnią. Prezes Zarządu przedstawił czego dotyczy spór prawny ze skarżącym, ponadto poinformował o fakcie złożenia przez Zarząd do Prokuratury Rejonowej zawiadomienia o podejrzeniu popełnienia przestępstwa przez skarżącego i jego żonę. Skarżący podniósł, iż w toku zebrania na Sali przebywały osoby nieupoważnione do przetwarzania danych. Z materiału zgromadzonego w sprawie wynikało, iż wszyscy uczestnicy ww. zgromadzenia posiadali legitymację do ich przetwarzania. W związku z powyższym, organ ds. ochrony danych osobowych w drodze decyzji administracyjnej[105] odmówił uwzględnienia wniosku skarżącego.

Jednocześnie z przedłożonej przez Spółdzielnię umowy powierzenia przetwarzania danych osobowych zawartej z Kancelarią prawną nie wynikał wprost cel, dla którego Spółdzielnia powierzyła Kancelarii przetwarzanie danych osobowych jej członków, jak i zakres danych, które mogły być przetwarzane, tj. nie zostało w niej wskazane jakie konkretnie kategorie (rodzaj) danych Spółdzielnia w ww. celu powierza Kancelarii. Ponadto z umowy ogólnie wynikało, iż dane przetwarzane będą przez Kancelarię w związku z wykonywaniem przez nią obsługi prawnej działalności Spółdzielni, a upoważnienie nadane Radcy prawnemu nie odnosiło się do przetwarzania danych osobowych członków Spółdzielni. Co prawda, brak prawidłowego upoważnienia, o którym mowa w art. 37 ustawy, nie przesądza o nielegalności przetwarzania danych przez osoby przetwarzające dane w imieniu tego podmiotu, to jednak nadanie takich upoważnienia świadczy o dochowaniu przez administratora danych obowiązku staranności przy przetwarzaniu danych i dbałości o właściwe zabezpieczenie danych. W związku z powyższym konieczne stało się skierowanie przez Generalnego Inspektora Ochrony Danych Osobowych wystąpienia do Spółdzielni celem wyeliminowania tych nieprawidłowości[106].

3.3.9. Oświata i szkolnictwo wyższe.

W omawianym okresie do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **51 skarg** dotyczących **oświaty**.

GIODO prowadził czynności wyjaśniające w związku ze skargą na udostępnienie osobom nieupoważnionym przez dyrektora jednej ze szkół danych osobowych małoletniego syna skarżącej zawartych w protokole powypadkowym. Skarżąca wskazała, iż ww. protokół został udostępniony rodzicom dzieci, którzy byli świadkami przedmiotowych zdarzeń. Organ

[105] Decyzja GIODO z dnia 5 listopada 2014 r. (DOLiS/DEC-1046/14/87040,87048,87055).
[106] Pismo GIODO z dnia 25 listopada 2014 r. (znak: DOLiS-440-1141/12/AZ/I/87036).

ustalił, iż ww. udostępnienie przez dyrektora szkoły danych osobowych małoletniego syna skarżącej zawartych w protokole powypadkowym na rzecz rodziców uczniów uczestniczących w wypadku odbyło się bez podstawy prawnej. Z uwagi jednak na fakt, że udostępnienie to było działaniem jednorazowym i działania takie nie były następnie kontynuowane, GIODO wydał decyzję[107] odmawiającą uwzględnienia wniosku.

Niezależnie od powyższego, Generalny Inspektor Ochrony Danych Osobowych, korzystając z uprawnienia przyznanego mu w art. 19 a ustawy o ochronie danych osobowych, zwrócił się do dyrektora zespołu szkół[108] o respektowanie przepisów o ochronie danych osobowych, w szczególności w odniesieniu do danych wrażliwych, bowiem takie działanie należało uznać za naruszające obowiązujące prawo ochrony danych. Dyrektor szkoły wyraził ubolewanie i wskazał, iż podjęte zostały działania mające na celu niedopuszczenie do podobnej sytuacji w przyszłości.

W innej ze skarg dotyczącej przetwarzania danych przez dyrektora biblioteki uniwersyteckiej, skarżący podniósł, iż biblioteka udostępniła jego dane na rzecz osoby nieuprawnionej, która następnie opublikowała te dane w Internecie. Skarżący podniósł zarzut nieprawidłowego zabezpieczenia przez bibliotekę danych osobowych. W toku postępowania przeprowadzonego przez GIODO zarzuty skarżącego dotyczące udostępnienia przez Dyrektora biblioteki jego danych osobowych na rzecz jakiejkolwiek osoby nieupoważnionej, nie potwierdziły się. Dyrektor biblioteki bowiem kategorycznie zaprzeczył, by kwestionowane w skardze udostępnienie danych skarżącego miało w ogóle miejsce, a ponadto oświadczył, iż w systemie bibliotecznym, w którym przetwarzane są dane osobowe, nie odnotowano faktu udostępnienia danych skarżącego na rzecz osób trzecich. Ponadto nie potwierdziły się również zarzuty skarżącego odnośnie niewłaściwego zabezpieczenia przez bibliotekę jego danych osobowych przetwarzanych w ww. systemie, bowiem Dyrektor biblioteki wykazał, że system ten spełniał wymogi właściwego zabezpieczenia, jak w szczególności zastosowano w nim środki techniczne w postaci szyfrowania danych przesyłanych pomiędzy serwerem a stacjami roboczymi i systemu alarmowego chroniącego dostęp do serwerowi, a także środki organizacyjne w postaci uaktualniana lista pracowników, którzy mają dostęp zdalny do systemu przetwarzającego dane osobowe czytelników i są upoważnieni do ich przetwarzania wraz z wyszczególnieniem przysługujących im uprawnień. Dlatego też brak było podstaw do tego, by dać wiarę twierdzeniom skarżącego, że jego dane „wyciekły" z biblioteki na skutek ich nienależytego zabezpieczenia przed udostępnieniem osobom trzecim. W związku z powyższym organ do spraw ochrony danych osobowych, w drodze decyzji administracyjnej, odmówił uwzględnienia wniosku[109].

---

[107] Decyzja GIODO z dnia 11 marca 2014 r. (DOLIS/DEC-207/14/18471,18473).
[108] Pismo GIODO z dnia 11 marca 2014 r. (znak: DOLiS-440-104/13/MKR/I/18470).
[109] Decyzja GIODO z dnia 6 maja 2014 r. (DOLiS/DEC-427/14/34406,34407).

3.3.10. Służba zdrowia.

W 2014 roku do Biura GIODO odnotowano **47 skarg** w sektorze dotyczącym **służby zdrowia**.

Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie administracyjne w sprawie skargi na udostępnienie danych osobowych przez jeden ze szpitali na rzecz szpitala specjalistycznego. Skarżący, w związku z wypadkiem jakiemu uległ, poddany został hospitalizacji w szpitalu wojewódzkim. W związku z koniecznością wykonania zabiegu artroskopii barku – którego to zabiegu nie wykonywał szpital wojewódzki – skarżacy został skierowany przez do szpitala Specjalistycznego w celu wykonania rzeczonego zabiegu. W skierowaniu wypisano dane osobowe Skarżacego w zakresie imienia, nazwiska, adresu zamieszkania i numeru PESEL. Skarżacy stawił się w izbie przyjęć szpitala specjalistycznego w celu poddania się ww. zabiegowi, udostępniając w tym celu swoje dane osobowe w zakresie imienia, nazwiska, daty urodzenia, numeru PESEL, numeru ubezpieczenia imienia i nazwiska żony, numeru telefonu i numeru telefonu żony. W przedmiotowej sprawie brak było dowodów wskazujących, że do kwestionowanego przez skarżącego udostępnienia danych osobowych doszło. Z wyjaśnień podmiotów jednoznacznie wynikało, że szpital wojewódzki nie udostępnił danych osobowych skarżącego na rzecz szpitala specjalistycznego, który to podmiot pozyskał dane osobowe skarżącego od niego samego, w związku ze zgłoszeniem się przez niego w celu wykonania zabiegu w ww. placówce. Na podstawie poczynionych ustaleń Generalny Inspektor wydał decyzję administracyjną, mocą której odmówił uwzględniania wniosku skarżącego[110]. W ustawowym terminie do Biura GIODO wpłynął wniosek skarżącego o ponowne rozpatrzenie sprawy zakończonej ww. decyzją. Po uzupełnieniu materiału dowodowego i ponownym rozpoznaniu sprawy organ ds. ochrony danych osobowych podtrzymał swoje stanowisko wyrażone w zaskarżonej decyzji[111].

3.3.11. Ubezpieczenia społeczne, majątkowe i osobowe.

W sektorze **ubezpieczeń społecznych, majątkowych i zdrowotnych** można odnotować znaczny wzrost liczby skarg kierowanych do Generalnego Inspektora. W 2014 r. do Biura GIODO wpłynęło **63 skarg** (dla porównania w 2013 r. było ich 37). W tej grupie stwierdzić można, że we wszystkich kategoriach wpływały skargi w zbliżonej ilości i dotyczyły one nieprawidłowości w procesie przetwarzania danych osobowych przez

[110] Decyzja GIODO z dnia 8 sierpnia 2013 r. (DOLiS/DEC-839/13/50482,50483,50485).
[111] Decyzja GIODO z dnia 21 lutego 2014 r. (DOLIS/DEC-170/14/14185,14192,14196).

towarzystwa ubezpieczeniowe polegające m.in. na przesyłaniu dokumentów dotyczących umowy ubezpieczenia osobom nieupoważnionym.

W 2014 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję odmawiającą uwzględnienia wniosku skarżących w sprawie ich skargi na przetwarzanie danych osobowych przez sąd okręgowy oraz Zakład Ubezpieczeń Społecznych[112]. ZUS przetwarzał dane osobowe skarżących, wyłącznie w celu prawidłowego ustalenia w stosunku do każdego z nich prawidłowej podstawy wymiaru składek na ubezpieczenia społeczne, w ramach merytorycznego rozstrzygnięcia w formie decyzji administracyjnej. Pomimo, że powyższe uczynione zostało w jednym akcie prawnym, a nie jak wskazują skarżący indywidualnie odnośnie każdego z nich, to na etapie wydawania ww. decyzji nie doszło do udostępnienia danych osobowych podmiotom nieuprawnionym. Przetwarzanie danych osobowych skarżących na potrzeby prowadzonego przez organ rentowy postępowania nastąpiło w oparciu o przesłankę, o której mowa w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych w związku z art. 34 ust. 3 ww. ustawy o systemie ubezpieczeń społecznych, który stanowi, że do informacji zawartych na kontach ubezpieczonych i kontach płatników składek oraz danych źródłowych będących podstawą zapisów na tych kontach stosuje się przepisy o ochronie danych osobowych. Jednocześnie Generalny Inspektor Ochrony Danych Osobowych nie stwierdził posiadania ustawowych kompetencji do oceny sposobu, w jaki ZUS rozstrzygnął w przedmiotowej sprawie, tj. że wydał decyzję dotyczącą zbiorczo wszystkich pracowników płatnika składek, a nie jak wskazywali skarżący w stosunku do płatnika składek w odniesieniu do każdego ze skarżących. Ocena tych okoliczności należała bowiem do organów odrębnych w trybie oceny instancyjnej.

W analizowanym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych przeprowadził również postępowanie administracyjne w sprawie skargi na udostępnienie przez jedno z towarzystw ubezpieczeniowych danych osobowych na rzecz spółki zajmującej się dochodzeniem roszczeń odszkodowawczych. W treści ww. skargi skarżąca podniosła w szczególności, iż w związku z toczącym się postępowaniem w sprawie dochodzenia roszczeń z tytułu doznanych przez nią obrażeń dłoni, towarzystwo ubezpieczeniowe odmówiło jej wypłaty odszkodowania, a w niedługim odstępie czasu otrzymała ona od spółki „ofertę dochodzenia roszczeń odszkodowawczych". Skarżąca dodała

[112] Decyzja GIODO z dnia 25 listopada 2014 r. (DOLiS/DEC-172/14/14218,14219,14220).

również, iż podpisując umowę z towarzystwem ubezpieczeniowym nie wyraziła zgody na przekazywanie jej danych osobowych „osobom postronnym". Odnosząc się do tego zarzutu skarżącej, wskazać należy, że nie znalazł on potwierdzenia w materiale dowodowym zebranym w toku postępowania wyjaśniającego przeprowadzonego w sprawie. Obie firmy zgodnie bowiem oświadczyły, iż źródłem danych osobowych skarżącej, które przetwarzała spółka w celu skierowania do niej oferty marketingowej, nie było towarzystwo ubezpieczeniowe. Wobec powyższego towarzystwu ubezpieczeniowemu nie można było postawić zarzutu naruszenia przepisów ustawy o ochronie danych osobowych[113].

3.3.12. Telekomunikacja.

W rozpatrywanych w 2014 r. sprawach dotyczących **telekomunikacji** do Biura GIODO wpłynęły **134 skargi** (dla porównania w 2013 r. było ich 86). Skargi te dotyczyły przetwarzania danych osobowych przez operatorów telekomunikacyjnych.

W analizowanym okresie Generalny Inspektor prowadził postępowanie w przedmiocie nakazania jednemu z operatorów telekomunikacyjnych usunięcia danych osobowych skarżącego utrwalonych na kopii dowodu osobistego oraz dokumentu prawa jazdy. W treści ww. skargi ustalono, iż skarżący udał się do salonu operatora w celu zawarcia umowy o świadczenie usług stacjonarnego Internetu. Pracownik salonu, z którym prowadził rozmowę, udzielił mu informacji, że wskazana umowa nie może być zawarta w związku ze sporem dotyczącym rozliczeń pomiędzy operatorem a spółką, w której skarżący był prezesem oraz którą reprezentował przy zawieraniu umowy o świadczenie usług. W związku z powyższym skarżący wezwał operatora do usunięcia nieprawidłowości w procesie przetwarzania danych osobowych poprzez zniszczenie kserokopii dowodu osobistego i usunięcie danych osobowych. Operator w odpowiedzi na pismo oświadczył, że zaprzestanie przetwarzania danych skarżącego, jednak nie potwierdził zniszczenia przekazanych kopii dokumentów. Spółka w związku z ww. umową pozyskała i przetwarzała dane osobowe skarżącego wynikające z kserokopii jego dowodu osobistego i prawa jazdy. W toku postępowania organ ds. ochrony danych osobowych ustalił, iż umowa, której dotyczy niniejsze postępowanie została zawarta ze spółką, w której skarżący był prezesem zarządu, nie zaś ze skarżącym jako osobą fizyczną. Dlatego też wszelkie informacje osobowe dotyczące jego osoby były zasadniczo zbędne dla przetwarzania ich w celach archiwizacji, bowiem to nie on był stroną ww. umowy. W ocenie organu przetwarzanie danych skarżącego jako osoby reprezentującej podmiot, z

[113] Decyzja GIODO z dnia 12 marca 2014 r. (DOLiS/DEC-225/14/18852,18854,18857).

którym zawarta była umowa o świadczenie usług telekomunikacyjnych, dla wykazywanego celu archiwalnego było zbędne. Tym samym ich przetwarzanie odbywało się z naruszeniem zasady adekwatności wyrażonej w art. 26 ust. 1 pkt 3 ustawy. W związku z powyższym Generalny Inspektor w drodze decyzji[114] nakazał ich usunięcie, zaś w pozostałym zakresie odmówił uwzględnienia wniosku. GIODO uznał ponadto, iż dane skarżącego w zakresie imienia, nazwiska, serii i numeru dowodu osobistego, numeru prawa jazdy oraz nr PESEL jako figurujące na umowie mogą być przetwarzane dla celów dowodowych (archiwalnych), jako dowód zawarcia ww. umowy przez oznaczoną osobę, o określonym numerze PESEL, reprezentującą abonenta, legitymującą się dwoma ww. oznaczonymi dokumentami. Te dane w sposób wystarczający identyfikują osobę skarżącego oraz dowodzą sposobu zawarcia przedmiotowej umowy, zatem stanowią wystarczające „potwierdzenie sposobu weryfikacji tożsamości Klienta". Skarżący domagał się również od Spółki zniszczenia kopii ww. dokumentów, natomiast – co wymaga podkreślenia – żaden przepis ustawy o ochronie danych osobowych nie przyznaje Generalnemu Inspektorowi kompetencji w zakresie podejmowania rozstrzygnięć, których przedmiotem jest nakaz usuwania dokumentów.

Ponadto organ do spraw ochrony danych osobowych przeprowadził postępowanie w sprawie wniosku Straży Miejskiej o nakazanie operatorowi telekomunikacyjnemu udostępnienia danych osobowych abonenta usług telekomunikacyjnych świadczonych przez spółkę, tj. użytkownika numeru telefonu, w zakresie jego imienia, nazwiska oraz adresu zamieszkania. Przedmiotowe dane były Straży Miejskiej niezbędne w celu ustalenia sprawcy wykroczenia, polegającego na umieszczaniu w miejscu publicznym do tego nie przeznaczonym ogłoszenia z numerem telefonu (art. 63a § 1 Kodeksu wykroczeń). Straż Miejska wykonywała zadania w zakresie ochrony porządku publicznego, zaś do wypełnienia zadania realizowanego dla dobra publicznego niezbędne było ustalenie sprawcy wykroczenia, a następnie skierowania do sądu wniosku o ukaranie. W związku z powyższym organ do spraw ochrony danych osobowych nakazał spółce udostępnienie na rzecz Straży Miejskiej żądanych przez nią danych[115].

3.3.13. Zatrudnienie.

W omawianym roku sprawozdawczym, do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęły **62 skargi**, w których zakwestionowano legalność działań -

[114] Decyzja GIODO z dnia 18 lutego 2014 r. (DOLiS/DEC-143/14/12420,12423).
[115] Decyzja GIODO z dnia 10 września 2014 r. (DOLiS/DEC-889/14/70777,70802).

sektorze **zatrudnienia**, tj. w procesie przetwarzania danych osobowych skarżących przez pracodawców, a w znacznej większości przez byłych pracodawców.

Przykładem może być skarga na udostępnienie danych osobowych skarżącego, zawartych w skierowanym do niego „liście otwartym" przez byłego pracodawcę, kontrahentom spółki. Skarżący poinformował, że we wskazanym liście została opisana jego sytuacja finansowa, rodzinna oraz stan jego zdrowia. Ponadto dodał, że w związku z faktem, iż skarżony podmiot ma status zakładu pracy powinien chronić jego dane, ze szczególnym naciskiem na dane dotyczące choroby. Zdaniem Generalnego Inspektora w niniejszej sprawie należało odnieść się do trzech zagadnień postawionych w skardze, a mianowicie do kwestii udostępnienia danych osobowych skarżącego w zakresie sytuacji rodzinnej, finansowej i jego stanu zdrowia. Ponadto w piśmie do kontrahentów wymienione zostały imiona córek skarżącego. W rozumieniu Generalnego Inspektora prawo każdego do ochrony dotyczących go danych świadczy o prawie ściśle związanym z tą osobą. Zatem powołania imion córek w tekście wskazanego listu nie można było uznać za daną osobową skarżącego, a wyłącznie danymi osobowymi wskazanych córek. Odnosząc się do zarzutu skarżącego w zakresie udostępnienia przez spółkę informacji o jego stosunkach majątkowych organ wskazał, że za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Ustawodawca za dane osobowe pozwala uznać tylko takie informacje, które umożliwiają ustalenie tożsamości osoby fizycznej. W związku z tym, że list został wysłany przez spółkę do 31 kontrahentów i zawierał imię, nazwisko skarżącego, jego adres, krótki opis jego przebiegu pracy w Spółce, a także informacje dotyczące gratyfikacji oraz pozapłacowych korzyści jakie skarżący otrzymywał od spółki, GIODO uznał je za informacje o stosunkach majątkowych skarżącego. Co zaś tyczy się udostępnienia przez spółkę informacji o stanie zdrowia organ uznał, iż nie znalazło ono uzasadnienia w żadnej z przesłanek wskazanych w art. 27 ust. 2 ustawy. Nie można było również uznać udostępnienia takich informacji jako mieszczących się w podstawie prawnej, którą przytoczył pełnomocnik spółki, tj. art. 27 ust. 2 pkt 2 ustawy w zw. z art. 94 pkt 9a kodeksu pracy (pracodawca jest obowiązany w szczególności prowadzić dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników). Zgodnie z art. 26 ust. 1 ustawy administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: (pkt 1) przetwarzane zgodnie z prawem, (pkt 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z

zastrzeżeniem ust. 2. W ocenie Generalnego Inspektora z uwagi na ww. okoliczności nie można było uznać, aby spółka, udostępniając dotyczące skarżącego informacje na rzecz kontrahentów, dołożyła szczególnej staranności, o której mowa w art. 26 ust. 1 ustawy. Organ uznał ponadto, iż spółka udostępniając dane osobowe skarżącego zrobiła to w sposób celowy, formułując i wysyłając listy do pewnego kręgu podmiotów[116]. Korzystając z uprawnienia wynikającego z art. 19a ustawy o ochronie danych osobowych, Generalny Inspektor, wskazując na zasady określone w art. 26 ustawy o ochronie danych osobowych, skierował do prezesa zarządu spółki wystąpienie[117] sygnalizując konieczność zmiany dotychczasowej praktyki i potrzebę poszanowania prawa do prywatności osób pracujących w Spółce.

3.3.14. Windykacja.

W roku 2014 do organu ds. ochrony danych osobowych wpłynęło **110 skarg** dotyczących sektora **windykacji** (dla porównania w roku 2013 było ich 92). Praktycznie wszystkie skargi w przedmiocie windykacji dotyczyły zbadania legalności pozyskania i przetwarzania danych osobowych przez firmy windykacyjne.

W jednej ze skarg skarżący wskazał, iż w związku z tym, że spółka wielokrotnie kontaktowała się z nim telefonicznie, próbował tą drogą, jak również drogą e-mailową ustalić podstawy przetwarzania jego danych przez ten podmiot. Jednakże spółka nie udzielała mu żadnych informacji bez podania przez niego pełnych danych osobowych. Skarżący podniósł również, iż skierował do spółki pismo, w którym bezskutecznie wnosił o udzielenie mu informacji, o których mowa w art. 32 ust. 1 pkt 1-5 ustawy o ochronie danych. Po przeprowadzeniu postępowania administracyjnego w niniejszej sprawie organ ds. ochrony danych osobowych dokonał ustaleń, iż dane osobowe skarżącego zostały przez spółkę usunięte. W związku z powyższym dalsze prowadzenie postępowania przez GIODO było bezprzedmiotowe[118]. Z uwagi jednak na to, iż w sprawie niewątpliwie doszło do nieprawidłowości w zakresie przetwarzania danych osobowych przez spółkę polegających na niedopełnieniu obowiązku informacyjnego, mimo prawidłowo doręczonego wniosku o jego spełnienie, o którym mowa w art. 33 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wystosował wystąpienie[119] w celu uczulenia spółki na aspekt legalności

[116] Decyzja GIODO z dnia 21 sierpnia 2014 r. (DOLiS/DEC-834/14/65100,65105).
[117] Pismo GIODO z dnia 21 sierpnia 2014 r. (znak: DOLiS-440-1397/13/KN/I/65122).
[118] Decyzja GIODO z dnia 14 maja 2014 r. (DOLiS/DEC-461/14/36725,36731).
[119] Pismo GIODO z dnia 14 maja 2014 r. (znak: DOLiS-440-960/13/AZ/I/36720).

przetwarzania danych osobowych i tym samym zapobieżenie podobnym nieprawidłowościom w przyszłości.

Inna skarga dotyczyła przekazania danych osobowych przez firmę ubezpieczeniową do firmy windykacyjnej. Spółki te zawarły ze sobą umowę o obsługę wierzytelności, której celem uczyniono dochodzenie wymagalnych roszczeń firmy ubezpieczeniowej. Skarżący wskazał, iż uregulował już zobowiązanie wobec firmy ubezpieczeniowej i wniósł o zbadanie legalności przetwarzania jego danych osobowych, w tym ich udostępnienia na rzecz firmy windykacyjnej. Organ ustalił, iż przetwarzanie danych skarżącego odbywało się wobec konieczności realizacji umowy zawartej z towarzystwem ubezpieczeniowym, co ma swoje oparcie w art. 23 ust. 1 pkt 3 ustawy. Z kolei podstawą prawną powierzenia przez firmę ubezpieczeniową na rzecz firmy windykacyjnej był przepis art. 31 ustawy. Celem powierzenia danych osobowych skarżącego była realizacja działań określonych umową powierzenia tj. m. in. obsługa dochodzenia wymagalnych wierzytelności administratora danych. W związku z powyższym organ do spraw ochrony danych osobowych odmówił uwzględnienia wniosku[120].

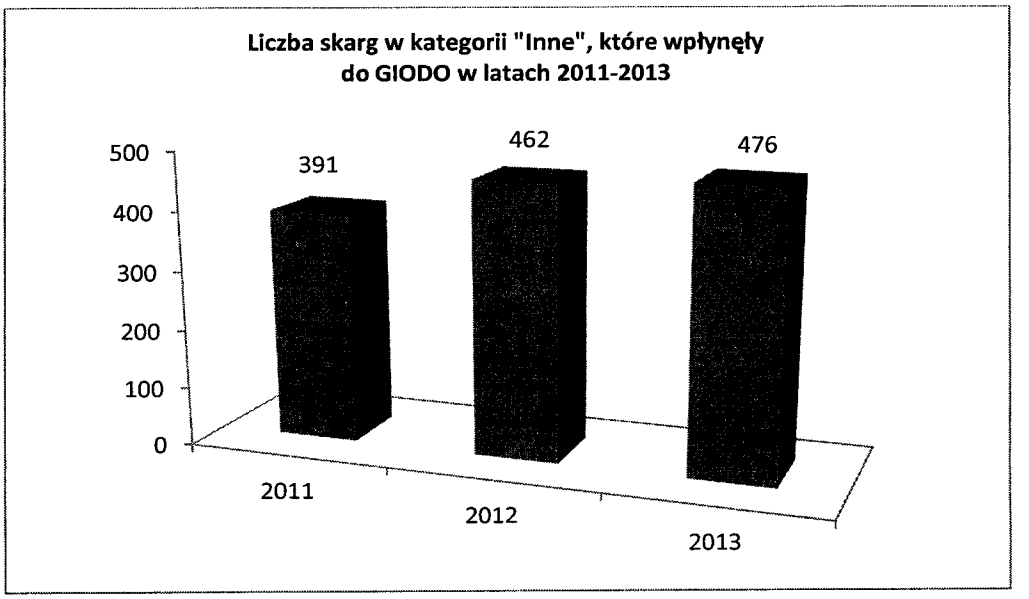
Ponadto organ prowadził postępowanie w sprawie przetwarzania danych osobowych skarżącej, w tym ich udostępnienia przez firmę telekomunikacyjną na rzecz firmy windykacyjnej. W toku postępowania administracyjnego organ ustalił, iż na podstawie umowy sprzedaży wierzytelności doszło do przeniesienia przez spółkę telekomunikacyjną wierzytelności, wynikających z umów o świadczenie usług telekomunikacyjnych (w tym umowy zawartej ze skarżącą), na ten podmiot windykacyjny i przekazania w związku z tym danych osobowych skarżącej. Na gruncie omawianej sprawy, przepisem prawa, z którego wynikał interes prawny w udostępnieniu danych osobowych skarżącej przez podmiot telekomunikacyjny na rzecz firmy windykacyjnej był art. 509 Kodeksu cywilnego, w myśl którego wierzyciel może bez zgody dłużnika przenieść wierzytelność na osobę trzecią (przelew), chyba że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania (§ 1). Wraz z wierzytelnością przechodzą na nabywcę wszelkie związane z nią prawa, w szczególności roszczenie o zaległe odsetki (§ 2). Ponadto GIODO uznał, iż dla legalności przetwarzania danych osobowych skarżącej w celu dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej przez firmę windykacyjną, wystarczało spełnienie przesłanki zawartej w przepisie art. 23 ust. 1 pkt 5 ustawy. Wobec powyższego i zgodniez przepisami o ochronie danych osobowych, niezasadne było postąpienie zgodnie z wnioskiem

[120] Decyzja GIODO z dnia 30 maja 2014 r. (DOLiS/DEC-511/14/41541,41543,41544).

skarżącej o usunięcie jej danych osobowych. W związku z czym organ, w drodze decyzji administracyjnej, odmówił uwzględnienia jej wniosku[121].

3.3.15. Inne.

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2014 r. wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej przedstawionych kategorii spraw. Ich liczba wyniosła **574.**



Wykres 16: ***Zestawienie porównawcze liczby skarg z sektora „Inne", które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2012–2014.***

W tym miejscu przede wszystkim należy wskazać, że w omawianym sektorze występowały – jak w latach poprzednich - skargi zawierający zarzut przetwarzania danych osobowych przez proboszczów **parafii Kościoła Katolickiego**. Jednak podkreślenia wymaga, iż w omawianym okresie sprawozdawczym sądy administracyjne po raz kolejny 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

[121] Decyzja GIODO z dnia 17 lipca 2014 r. (DOLiS/DEC-675/14/55188,55189,55191,55193,55195,55196).

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 złożonego przez nich „oświadczeń woli" o wystąpieniuz Kościoła, skutecznie z niego wystąpiły. W pierwszych orzeczeniach, w analogicznych sprawach, NSA uznawał, iż powyższa ocena powinna być dokonywana w oparciu o wewnętrzne przepisy Kościoła Katolickiego[122]. W związku z czym 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[123] NSA 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, jak również 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 lub umarzał postępowanie, jeśli dane zostały sprostowane w toku postępowania toczącego się przed GIODO. Wojewódzki Sąd Administracyjny w Warszawie wyrokiem[124] uchylił zaskarżoną decyzję GIODO[125] i poprzedzającą ją decyzję. WSA podkreślił, że w polskim prawie jest mocno ugruntowana zasada uprzedniego rozstrzygania sporu pomiędzy obywatelem a daną organizacją na zasadzie prawa wewnętrznego tej organizacji. „W niniejszej sprawie Generalny Inspektor rażąco uchybił tej zasadzie, wkraczając z rozstrzygnięciem stanowczym

[122] M. in. 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).

[123] M. in. 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).

[124] Wyrok WSA w Warszawie z dnia 21 sierpnia 2014 r. (sygn. akt II SA/Wa II SA/Wa 389/14).

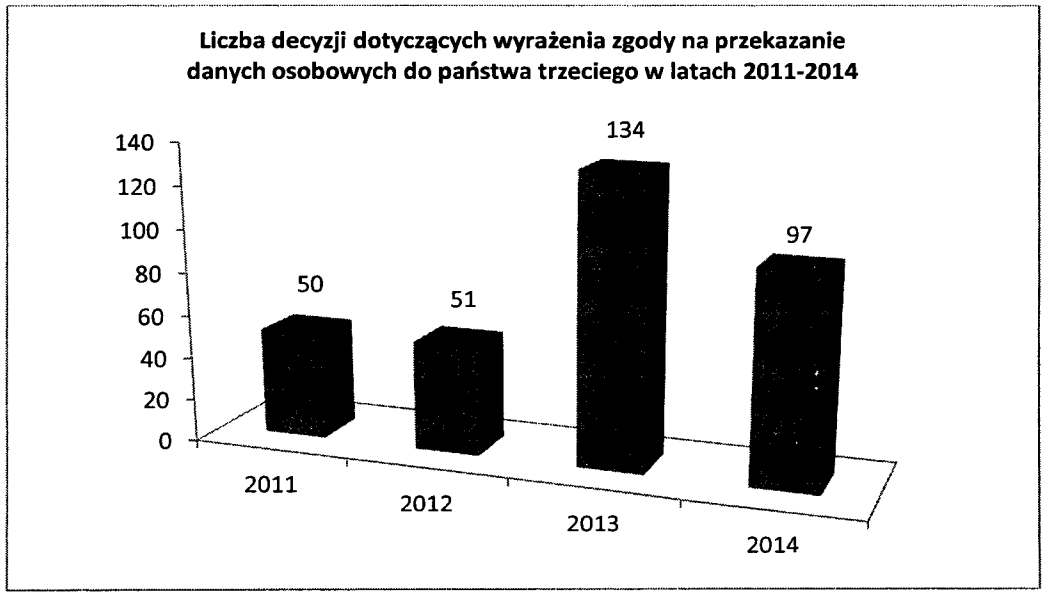
[125] Decyzja GIODO z dnia 8 stycznia 2014 r. (DOLiS/DEC-5/14/943,948).

w sprawie, która powinna zostać załatwiona zgodnie z Kodeksem Prawa Kanonicznego". Od ww. wyroku organ ds. ochrony danych osobowych złożył skargę kasacyjną, która aktualnie oczekuje na rozpatrzenie przez Naczelny Sąd Administracyjny, zaś niniejsze stanowisko WSA jest powielane w kolejnych wyrokach WSA[126].

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).

Ogółem Generalny Inspektor wydał w 2014 r. 97 decyzji administracyjnych dotyczących przekazania danych osobowych do państw trzecich[127]. Niemniej należy zaznaczyć, że część decyzji została wydana w postępowaniach administracyjnych, które zostały zainicjowane w poprzednich latach. Należy również zaznaczyć, że w związku z nowelizacją art. 48 ustawy, która weszła w życie w dniu 1 stycznia 2015 r., omawiany rok sprawozdawczy był ostatnim, w którym Generalny Inspektor wydawał decyzje w dotychczasowym modelu.



[126] M.in. wyrok WSA w Warszawie z dnia 20 maja 2015 r. (sygn. akt II SA/Wa 1604/14).

[127] Zgodnie z art. 48 ustawy, 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.

Wykres 17: ***Zestawienie porównawcze liczby decyzji dotyczących wyrażenia zgody na przekazanie danych osobowych do państwa trzeciego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2011-2014.***

Przeważająca większość prowadzonych przez Generalnego Inspektora postępowań administracyjnych została zakończona wydaniem decyzji wyrażającej zgodę na przekazanie danych do państwa trzeciego. W 2014 r., podobnie jak w latach poprzednich, pojawiały się postępowania, które wymagały umorzenia w całości bądź w części ze względu na swoją bezprzedmiotowość spowodowaną tym, że państwa, do których miały być przekazane dane osobowe zapewniały odpowiedni poziom ochrony danych osobowych[128], co zostało potwierdzone odpowiednimi decyzjami Komisji Europejskiej wydanymi na mocy art. 25 ust. 6 dyrektywy 95/46/WE. W konsekwencji, Generalny Inspektor wydawał decyzje o umorzeniu postępowania w odniesieniu do przekazania danych do takich importerów. Należy zaznaczyć, że również transfer danych do odbiorców w Stanach Zjednoczonych Ameryki, którzy należeli do programu „bezpiecznej przystani", nie wymagał uzyskania zgody Generalnego Inspektora[129].

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. 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 wpływał na zakres oceny dokonywanej przez GIODO. Należy bowiem pamiętać, że organ ochrony danych osobowych był obowiązany uznać taki instrument prawny za zapewniający odpowiednie gwarancje praw i wolności osób, których dane dotyczą. W toku postępowania administracyjnego weryfikacji podlegała 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.

---

[128] 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

[129] W dniu 6 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej w swoim orzeczeniu w sprawie C-362/14 Maximillian Schrems vs. Data Protection Commissioner stwierdził nieważność decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r. przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, 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 USA (Dz.Urz. WE L 215 z 28.8.2000).

W odniesieniu zaś do zakresu oceny wprowadzonych w państwie trzecim zabezpieczeń danych osobowych, a co za tym idzie zakresu żądanych od wnioskodawcy informacji o zastosowanych środkach organizacyjno – technicznych, to była ona uzależniona od rodzaju klauzul. W sytuacji zastosowania obydwu zestawów klauzul znajdujących zastosowanie do przekazania danych pomiędzy administratorami, było 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 oznaczało, 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 była zgodność zastosowanych środków z przepisami ww. rozporządzenia. Niemniej nadal możliwy był 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 poprzednim okresie sprawozdawczym GIODO w 2014 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.

Należy również zauważyć, że w kolejnych latach liczba zgód wydanych przez Generalnego Inspektora powinna radykalnie zmaleć, gdyż od 1 stycznia 2015 r. nie są one wymagane w sytuacji zastosowania standardowych klauzul umownych zatwierdzonych przez Komisję Europejską. Natomiast w odniesieniu do WRK znowelizowany art. 48 ustawy, przewiduje nową instytucję, tj. zatwierdzenie wiążących reguł korporacyjnych.

W tym miejscu należy przypomnieć, iż w dniu 1 stycznia 2015 r. weszły w życie, wprowadzone na mocy art. 9 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej, zmiany art. 48 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, dotyczące **zwolnienia z obowiązku uzyskania zgody GIODO na przekazywanie danych osobowych do państwa trzeciego**, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, gdy ich przekazywanie odbywa się na podstawie **standardowych klauzul umownych** albo **wiążących reguł korporacyjnych**. Nowe przepisy wprowadzają w polskim porządku prawnym instytucję wiążących reguł korporacyjnych oraz określają tryb ich zatwierdzenia przez GIODO. Przyjęte rozwiązania mają na celu przygotowanie administratorów danych do unormowań zapowiadanych w projekcie 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 osobowych) [COM(2012) 11, Dz. Urz. UE C 102 z dnia 5 kwietnia 2012 r., s. 24].

Standardowe klauzule umowne zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 95/45/WE będzie można stosować w umowach z podmiotami z państw trzecich. Wiążące reguły korporacyjne natomiast dotyczyć będą podmiotów należących do tej samej grupy przedsiębiorców (tej samej grupy kapitałowej). Wiążące reguły korporacyjne mogą być stosowane po ich zatwierdzeniu przez GIODO (w drodze decyzji administracyjnej), po przeprowadzeniu nieobowiązkowych konsultacji z organami ochrony danych osobowych państw Europejskiego Obszaru Gospodarczego, na których terytorium mają siedziby przedsiębiorcy należący do ww. grupy. Jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia ww. organu ochrony danych, GIODO może je uwzględnić.

Podkreślenia wymaga fakt, iż przepisy art. 47 i 48 ustawy wprowadzają jedynie dodatkowe wymogi, które należy spełnić, gdy zamierza się przekazywać dane osobowe do państwa trzeciego. Z tego względu administrator danych jest zobowiązany spełnić wszystkie obowiązki nałożone przez ustawę. Poza posiadaniem podstawy prawnej do przetwarzania określonych kategorii danych, administrator danych musi m.in. zapewnić, aby ich zakres był

dopuszczalny w świetle powszechnie obowiązujących na terytorium Rzeczypospolitej Polskiej przepisów prawa. Jednocześnie w przypadku kwalifikowanej formy przetwarzania danych, jaką jest przekazanie danych do innego administratora danych, który ma siedzibę w państwie trzecim, zachodzi konieczność spełnienia jednej z przesłanek legalności przetwarzania danych, wymienionych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy.

4. Rozpatrywanie zawiadomień o naruszeniu danych osobowych.

Na mocy przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.) dostawcy publicznie dostępnych usług telekomunikacyjnych - w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych zobowiązani są w szczególności powiadomić o tym właściwy organ ds. ochrony danych osobowych (GIODO).

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, wyznaczeni przez Generalnego Inspektora pracownicy Biura GIODO wykonują zadanie organizacji i koordynacji 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.[130]

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 2014 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **155 zawiadomień o naruszeniu danych osobowych.**

Ponadto w analizowanym 2014 r. odbyło się kolejne trzecie już spotkanie (2 poprzednie odbyły się w 2013 r.) informacyjno – edukacyjne GIODO z przedstawicielami dostawców publicznie dostępnych usług telekomunikacyjnych, podczas którego poruszono m.in. kwestie dotyczące aktualnych problemów omawianych na gruncie europejskim (w szczególności dotyczących uzgodnień co do wspólnego formularza zgłoszeniowego, kwestii naruszeń ponadkrajowych, utraty danych zanonimizowanych oraz przetwarzania danych

[130] 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.

telekomunikacyjnych), zmiany procedur w kierunku pełnej elektronizacji postępowania w sprawie zgłaszania naruszeń oraz ewentualnej eliminacji zdarzeń dotyczących pojedynczych naruszeń.

Warte podkreślenia jest również zaangażowanie pracowników Biura GIODO odpowiedzialnych za tę część działalności Biura w organizowane w 2014 roku warsztaty dotyczące naruszeń ochrony danych w sektorze telekomunikacyjnym, mianowicie:

1) 1st pan-European Personal Data Breach Excercise – projekt realizowany przez Komisję Europejską polegający na praktycznej symulacji scenariusza ogólnoeuropejskiego naruszenia ochrony danych w sektorze telekomunikacyjnym. Zasadniczym celem projektu było przygotowanie wspólnego mechanizmu działania organów ochrony danych osobowych w UE w obliczu takiego naruszenia. W projekcie oprócz Polski, reprezentowanej przez przedstawicieli GIODO, uczestniczyło 6 państw: Francja, Niemcy, Grecja, Irlandia, Włochy i Hiszpania.
2) Cyber-EXE Polska 2014 – projekt realizowany przez Fundację Bezpieczna Cyberprzestrzeń w partnerstwie m.in. z Rządowym Centrum Bezpieczeństwa i pod patronatem Ministerstwa Administracji i Cyfryzacji. Ćwiczenia „Cyber-EXE Polska 2014" skierowane były do firm z sektora telekomunikacyjnego. Zasadniczym celem ćwiczenia było zbadanie zdolności i przygotowania organizacji do identyfikacji zagrożeń w obszarze bezpieczeństwa teleinformatycznego, odpowiedzi na te zagrożenia oraz skutecznej współpracy w ramach sektora telekomunikacyjnego. Wśród podmiotów administracji publicznej uczestniczących w ćwiczeniach znalazły się: Biuro Generalnego Inspektora Ochrony Danych Osobowych, Komenda Główna Policji, Ministerstwo Administracji i Cyfryzacji, Urząd Komunikacji Elektronicznej oraz Rządowe Centrum Bezpieczeństwa.

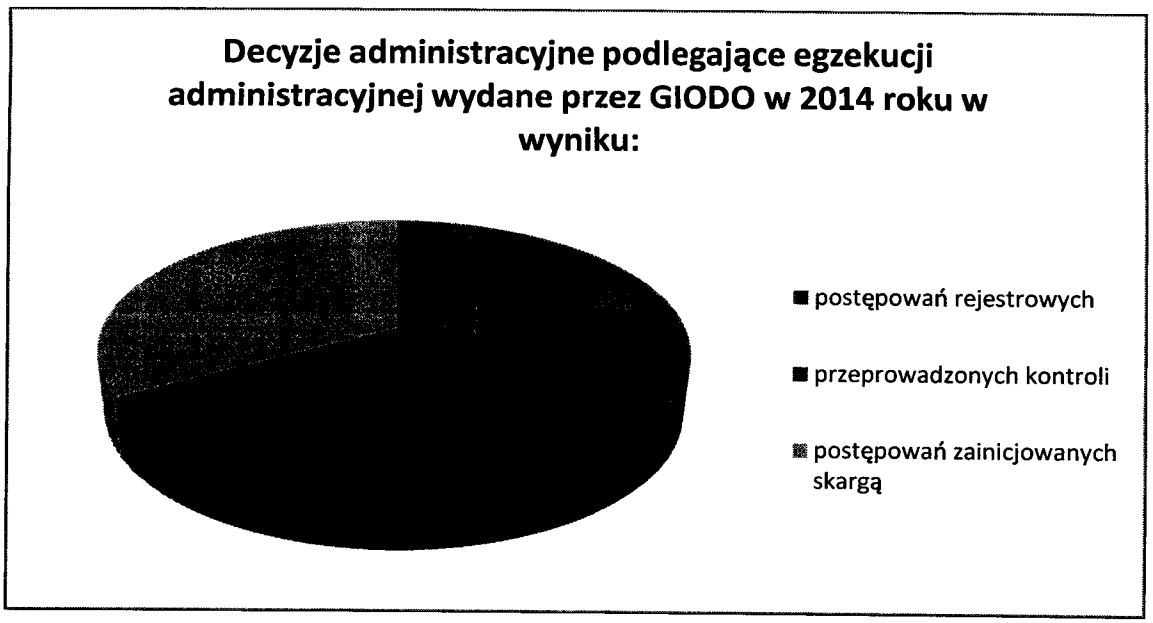
5. Egzekwowanie obowiązków o charakterze niepieniężnym określonych w decyzjach administracyjnych GIODO.

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.). By to zadanie realizować Generalny Inspektor został uznany za organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym, a obowiązki z zakresu ochrony danych osobowych, nakładane w drodze decyzji Generalnego Inspektora zostały dodane do katalogu obowiązków podlegających egzekucji administracyjnej.

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 2014 r. Generalny Inspektor wydał **123 decyzje administracyjne** zawierające nałożony na strony nakaz (obowiązek) do wykonania i **podlegających egzekucji administracyjnej**. Spośród decyzji wydanych w 2013 r. **56** (46 %) dotyczyło postępowań rejestrowych, **26** (21 %) zostało wydanych w związku z przeprowadzonymi kontrolami, **41** (33 %) wydano na skutek postępowania zainicjowanego skargą.

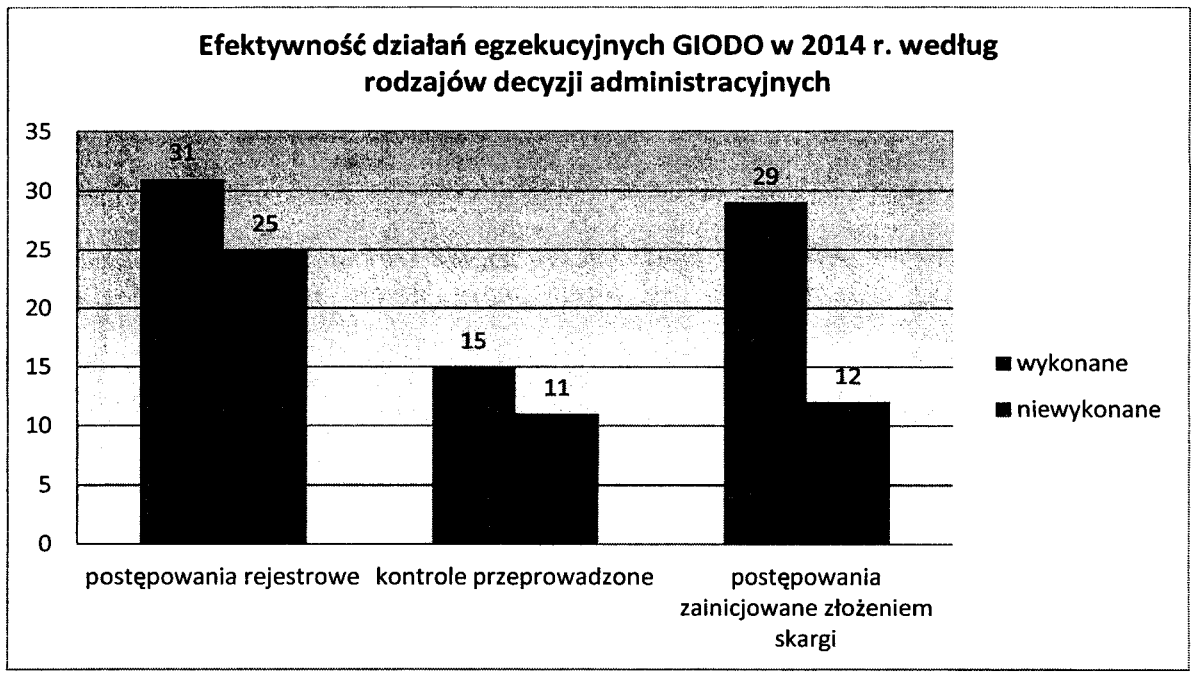


Wykres 18: ***Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji, wydanych przez GIODO w 2014 r.***

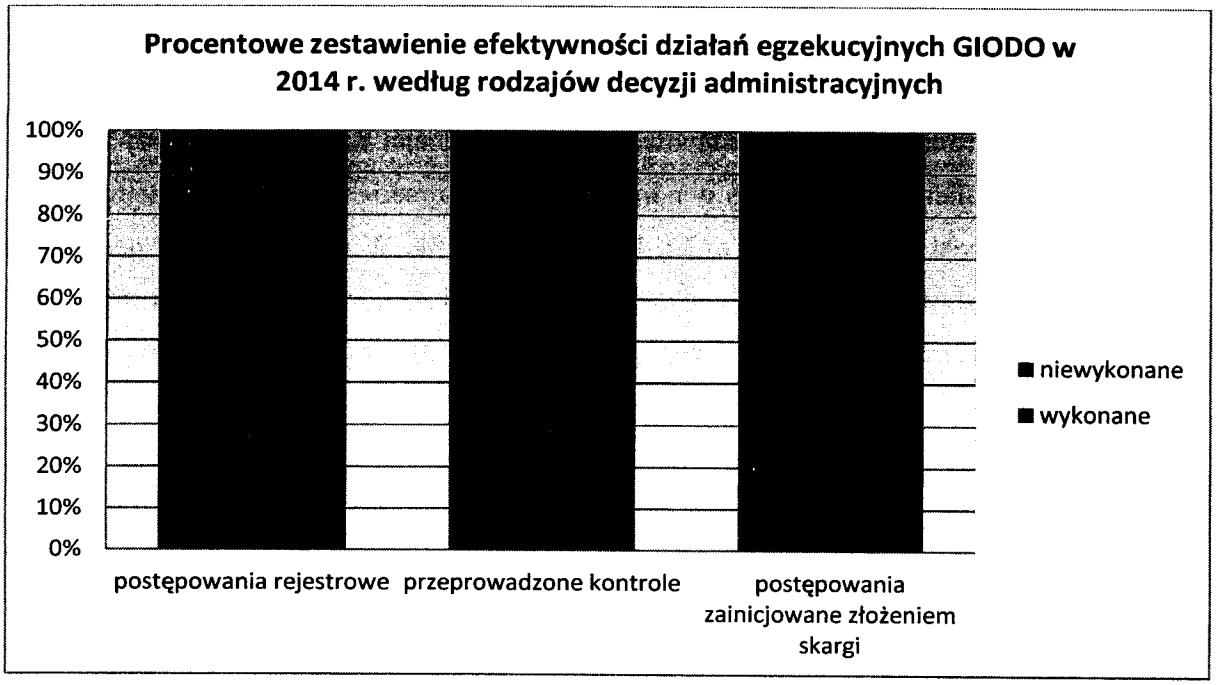
Efektywność prowadzonych w 2014 r. przez Generalnego Inspektora działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków, przedstawia się następująco: spośród 123 decyzji administracyjnych **wykonanych zostało przez zobowiązanych 75 decyzji**, 48 decyzji na koniec 2014 r. pozostało niewykonanych. Decyzje te objęte są działaniami egzekucyjnymi w 2015 r. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań Generalnego Inspektora Ochrony Danych Osobowych oraz przeprowadzonych kontroli sprawdzających. W 15 przypadkach wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia zobowiązani w 6 przypadkach wykonali w całości decyzję administracyjną GIODO.

Wobec 3 zobowiązanych prowadzone było postępowanie egzekucyjne wszczęte jeszcze w 2013 r. na podstawie wystawionych tytułów wykonawczych, z zastosowaniem środka egzekucyjnego w postaci nałożenia grzywny w celu przymuszenia (w obu przypadkach wysokość grzywny wyniosła 25.000 zł). W jednym przypadku postępowanie egzekucyjne zostało w 2014 r. zakończone, w związku z wykonaniem przez zobowiązanego w całości obowiązku zawartego w tytule wykonawczym. Dwa postępowania egzekucyjne nie zostały zakończone w 2014 r. i będą kontynuowane w 2015 r.

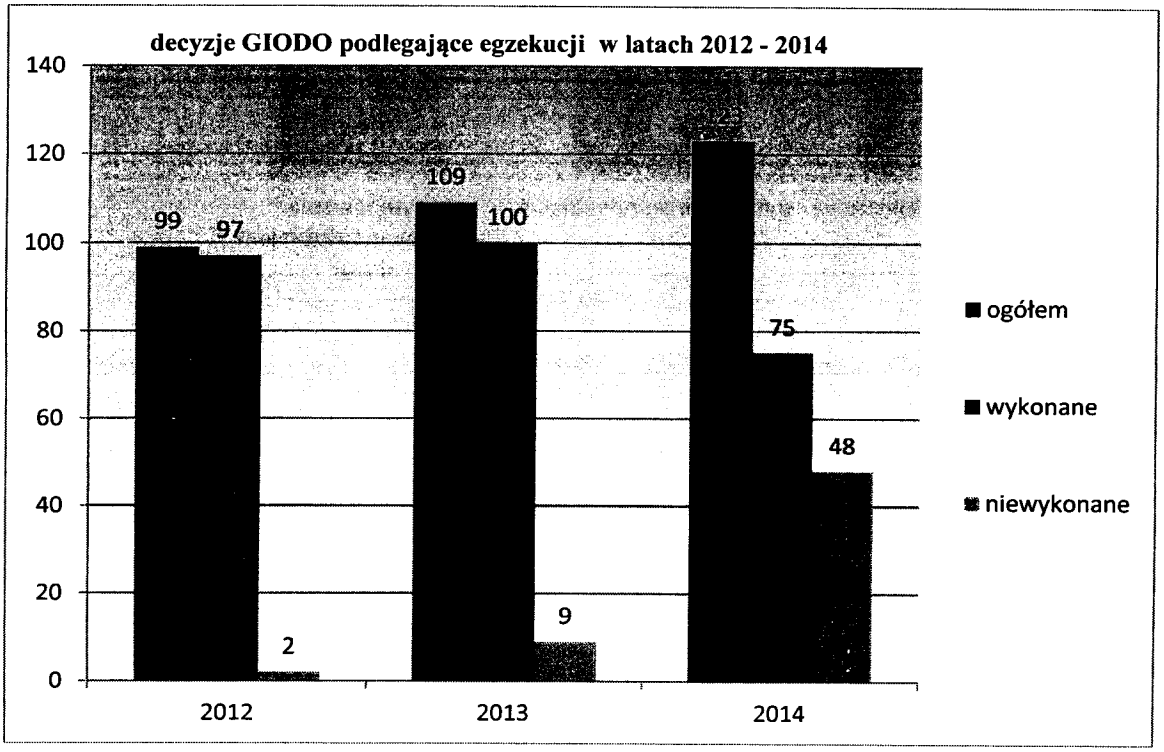
Spośród decyzji wydanych w 2014 r. i wykonanych przez zobowiązanych w 2014 r. **31** dotyczyło postępowań rejestrowych, **15** zostało wydanych w związku z przeprowadzonymi kontrolami, **29** wydano na skutek postępowania zainicjowanego skargą. Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w 2014 r. wynosił **61%.** W odniesieniu do postępowań rejestrowych efektywność egzekucji wynosiła **55%**, wobec decyzji wydanych w związku z przeprowadzonymi kontrolami - **58%**, natomiast w stosunku do decyzji wydanych na skutek postępowań zainicjowanych skargą - **71%**.



Wykres 19: ***Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2014 r.***



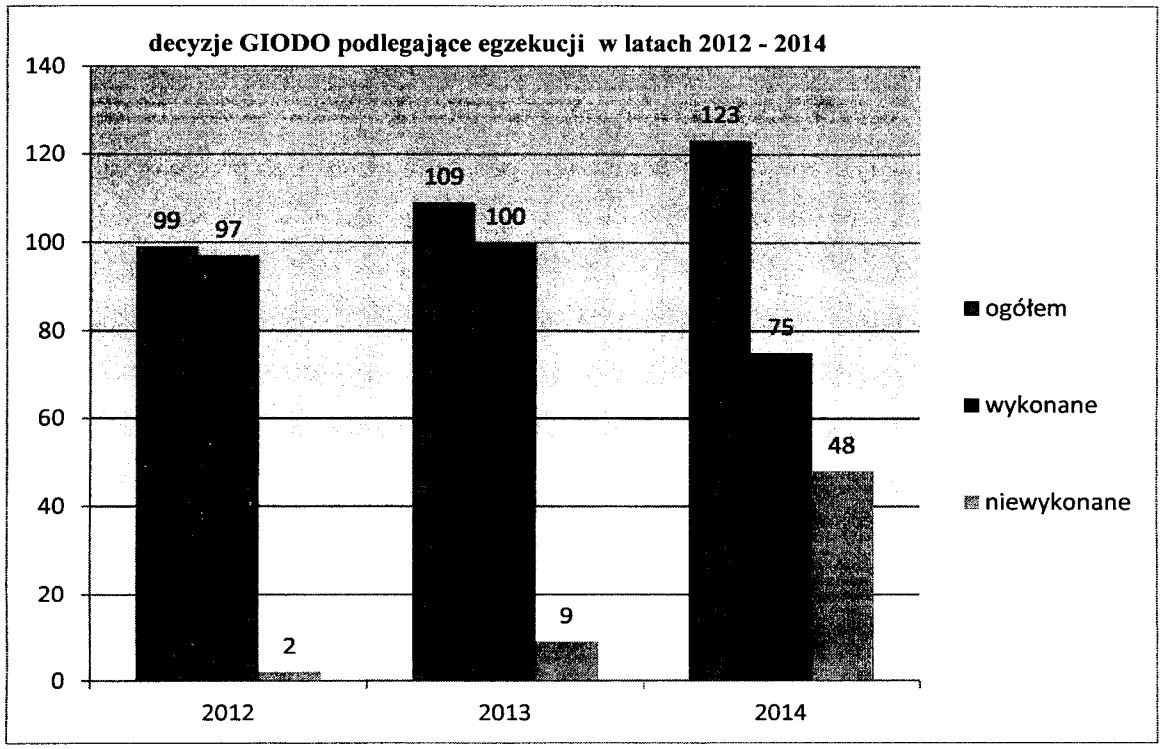
Wykres 20: ***Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2014 r.***



Wykres 21. ***Zestawienie decyzji GIODO podlegających egzekucji administracyjnej i efektywność podejmowanych działań egzekucyjnych w latach 2012 – 2014.***

Na przestrzeni lat 2012-2014 można zaobserwować systematyczny wzrost liczby decyzji GIODO podlegających egzekucji administracyjnej. W 2012 r. wydanych zostało 99 takich decyzji, zaś w 2013 r. było ich 109, co stanowi wzrost o 10%. Natomiast w 2014 r. Generalny Inspektor Ochrony Danych Osobowych wydał 123 decyzje administracyjne podlegające egzekucji administracyjnej, co stanowi wzrost o 13% w stosunku do roku poprzedniego.

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w latach 2012-2014 przedstawia się następująco: spośród decyzji GIODO objętych egzekucją administracyjną w 2012 r. efektywność wynosiła **98%,** w odniesieniu do postępowań egzekucyjnych prowadzonych w 2013 r. efektywność egzekucji kształtowała się na poziomie **92%**, natomiast w odniesieniu do 2014 r. - **61%.** Niższy wskaźnik efektywności w odniesieniu do 2014 r. wynikał z faktu, iż wobec tych decyzji działania egzekucyjne zostały rozpoczęte, zobowiązani sukcesywnie wykonywali nakazy zawarte w decyzjach i byli w trakcie składania informacji o wykonaniu decyzji do Generalnego Inspektora.



Wykres 22: ***Zestawienie liczby decyzji GIODO podlegających egzekucji administracyjnej i efektywność podejmowanych działań egzekucyjnych w latach 2012 – 2014.***

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[131].

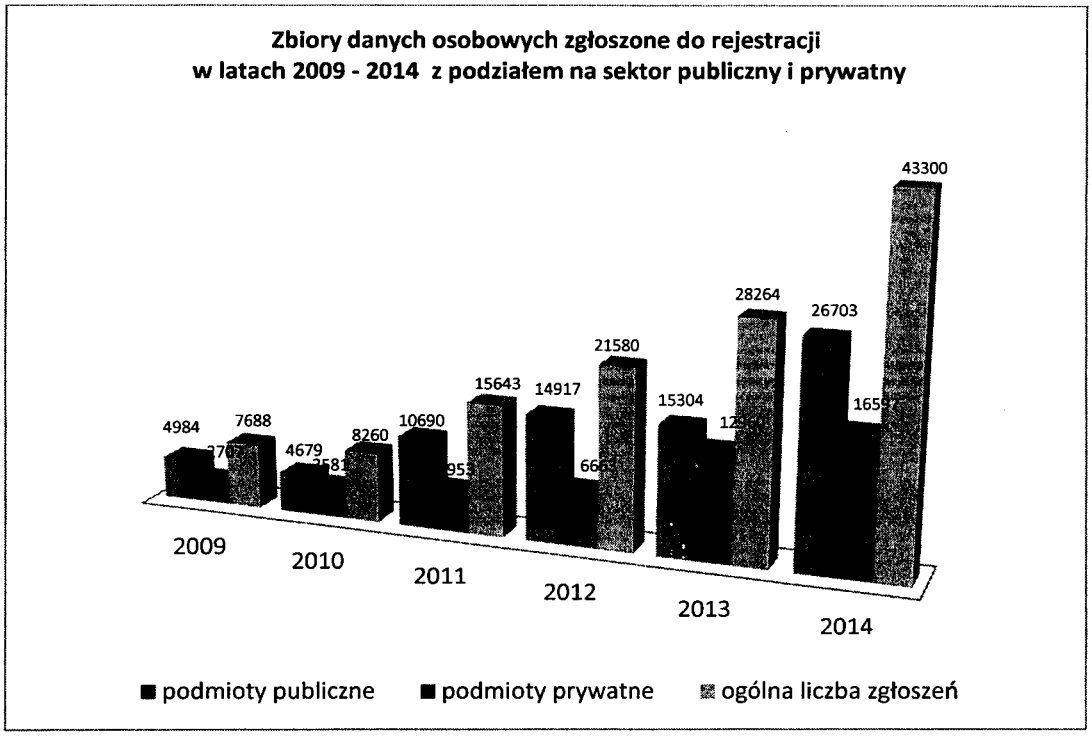
Głównym celem rejestracji zbiorów danych osobowych jest zapewnienie przejrzystości w sferze przetwarzania danych osobowych oraz stworzenie warunków do sprawowania indywidualnej oraz urzędowej kontroli nad przestrzeganiem zasad przyjętych w ustawie o ochronie danych osobowych. Prowadzenie ogólnokrajowego 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.

Kontrola wstępna procesów przetwarzania danych jest szczególnie istotna w przypadku zbiorów, do których administrator ma zamiar pozyskiwać dane szczególnie chronione. Na podstawie przesłanego przez administratora danych zgłoszenia, Generalny Inspektor Ochrony Danych Osobowych ocenia przestrzeganie przez administratora danych zasad przetwarzania danych osobowych, w tym również to czy istnieje podstawa prawna do przetwarzania danych osobowych, czy pozyskiwane są wyłącznie dane adekwatne do celu przetwarzania, a także spełnienie podstawowych wymogów w zakresie zabezpieczenia przetwarzanych danych osobowych. Odmawiając rejestracji zbioru danych, Generalny Inspektor Ochrony Danych Osobowych nakazuje usunięcie uchybień w procesie przetwarzania danych oraz ograniczenie przetwarzania danych wyłącznie do ich przechowywania do czasu zarejestrowania zbioru po jego ponownym zgłoszeniu, co następuje po usunięciu wad, które były powodem odmowy rejestracji.

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

[131] Od dnia 1 stycznia 2015 r. Generalny Inspektor Ochrony Danych Osobowych, zgodnie z art. 12 pkt 4 oraz art. 46c ustawy o ochronie danych osobowych, prowadzi ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji i udziela informacji o zarejestrowanych administratorach bezpieczeństwa informacji. Zadania te realizowane są przez Departament Rejestracji Zbiorów Danych Osobowych.

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 2014 roku, administratorzy danych, wypełniając obowiązek określony w art. 40 ustawy o ochronie danych osobowych[132], **zgłosili do rejestracji** Generalnemu Inspektorowi Ochrony Danych Osobowych **43300 zbiorów (w 2013 - 28264 zbiory)**, z czego podmioty z sektora administracji publicznej zgłosiły 26703 zbiory (w 2013 -15304 zbiory), co stanowiło 62 % ogólnej liczby zgłoszeń dokonanych w tym okresie, zaś podmioty z sektora prywatnego 16597 zbiorów (w 2013 - 12960 zbiorów), co stanowiło 38 % ogólniej liczby zgłoszonych zbiorów.



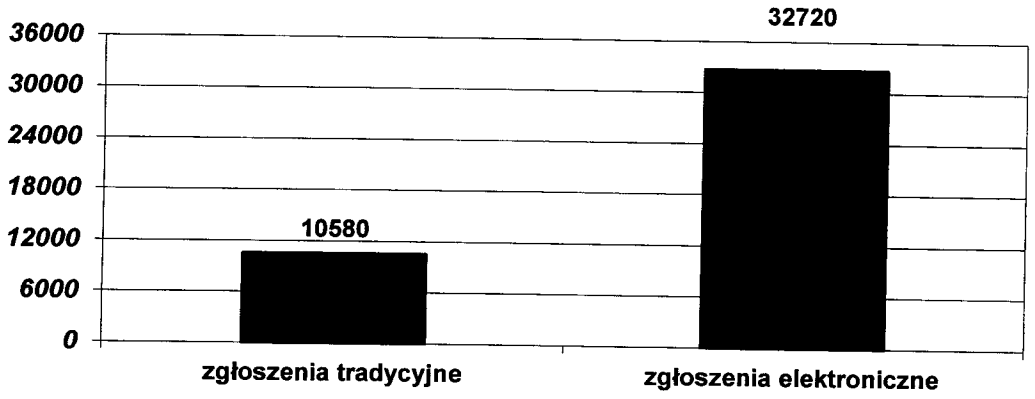
Wykres 23: ***Liczbowe zestawienie zbiorów danych osobowych zgłoszonych do rejestracji przez podmioty publiczne i prywatne w latach 2011 - 2014.***

Analizując powyższy wykres należy zauważyć **bardzo duży wzrost (w stosunku do roku 2013 o 53 %, w stosunku do roku 2012 o 101 %, zaś w stosunku do roku 2011 o 177 %) liczby zgłoszeń nadesłanych do rejestracji w 2014 roku.** W liczbach bezwzględnych

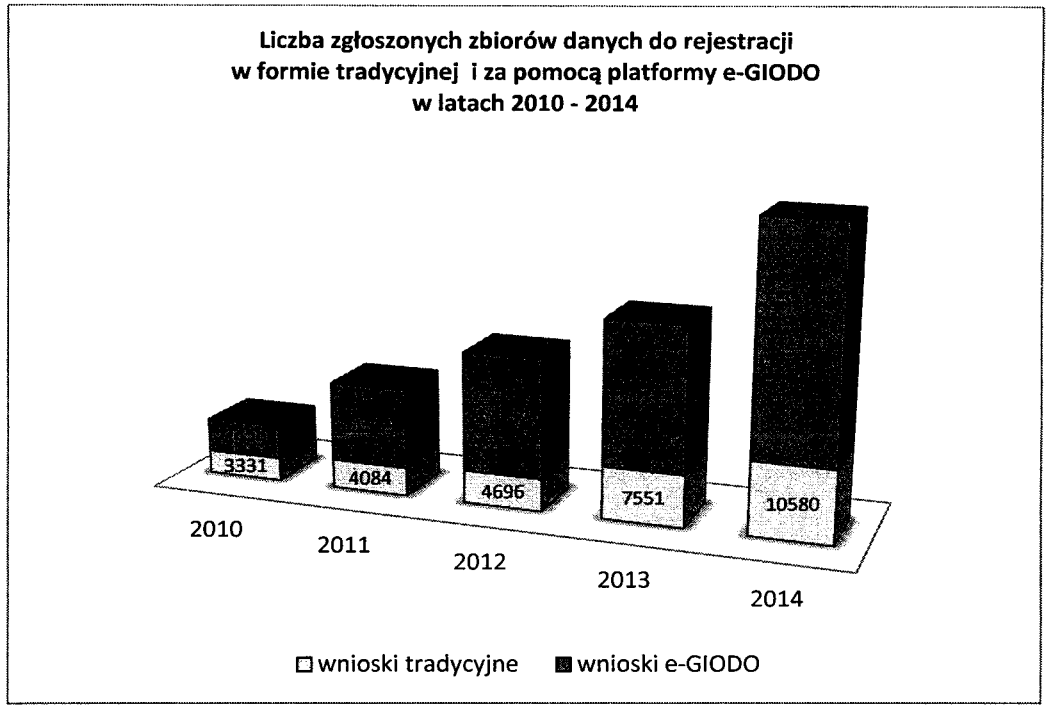
[132] Zgodnie z art. 40 ustawy, w brzmieniu obowiązującym przed dniem 1 stycznia 2015 r., administrator danych obowiązany jest zgłosić zbiór danych do rejestracji, z wyjątkiem przypadków określonych w art. 43 ust. 1 ustawy.

oznacza to, że w omawianym roku do Biura GIODO wpłynęło ponad 15000 zgłoszeń więcej, niż w roku go poprzedzającym i ponad 27600 zgłoszeń więcej, niż w roku 2011. Ponadto należy wskazać, że nastąpił duży wzrost liczby zgłoszeń zbiorów pochodzących od podmiotów publicznych – o 74 % w stosunku do roku 2013, podczas gdy wzrost zgłoszeń składanych przez podmioty z tej grupy w 2013 roku wynosił tylko 3 %. Mniej dynamiczny był wzrost liczby zgłoszeń złożonych przez podmioty prywatne, który wyniósł 28 %. W konsekwencji w roku sprawozdawczym 2014 od podmiotów prywatnych pochodziło 38 % ogólnej liczby zgłoszeń, podczas gdy w 2013 roku odsetek ten wynosił 46 %.

W roku 2014 roku **przy użyciu programu wspomagającego (eGIODO)**, udostępnionego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych, **zgłoszono do rejestracji 32720 zbiorów danych.** Dla porównania, w 2013 r. liczba ta wynosiła 20713 zbiorów. Zgłoszenia dokonane drogą elektroniczną stanowiły 75 % wszystkich zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2014 r. Jest to wynik porównywalny do poprzednich okresów sprawozdawczych (2013 – 73 %, 2012 – 78 %, 2011 – 74 %).



Wykres 24: ***Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonanych w 2014 r. w formie tradycyjnej i elektronicznej.***

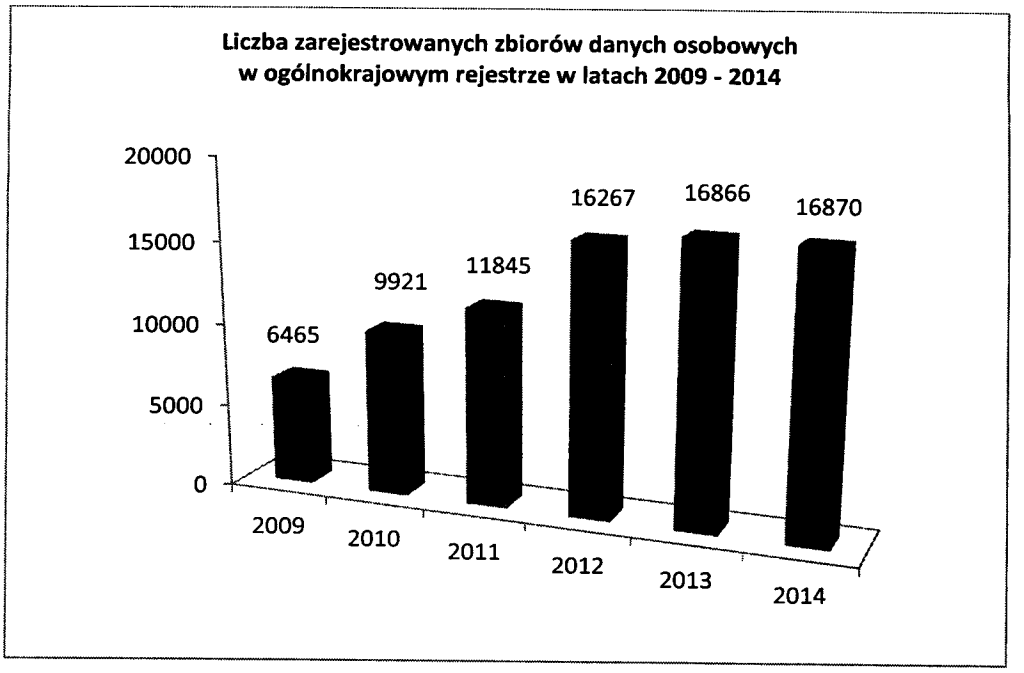


Wykres 25: ***Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2009 - 2014 r. w formie tradycyjnej i przy użyciu elektronicznego programu wspomagającego, udostępnionego na stronie www.giodo.gov.pl***

Liczba **zakończonych postępowań** prowadzonych w związku ze zgłoszeniami zbiorów do rejestracji w okresie sprawozdawczym wyniosła **18470, tj. o 586 więcej niż w roku 2013, o 1399 więcej niż w roku 2012 i o 5872 więcej niż w 2011 r.**

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 16870 zbiorów danych.**



Wykres 26: ***Zestawienie porównawcze zarejestrowanych zbiorów danych osobowych w ogólnokrajowym rejestrze w latach 2008 - 2014.***

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 z późn. zm.). W konsekwencji w 2014 roku skierowano do wnioskodawców, na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego, **781 wezwań do uzupełnienia w zgłoszeniu braków formalnych**.

W wielu przypadkach informacje zawarte w zgłoszeniu nie pozwalały na zakończenie sprawy bez przeprowadzenia **postępowania wyjaśniającego**. W 2014 roku w toku postępowań rejestracyjnych skierowano do wnioskodawców **1674 pisma,** w których Generalny Inspektor Ochrony Danych Osobowych zwracał się o złożenie pisemnych wyjaśnień oraz informował o uprawnieniach strony przed wydaniem decyzji administracyjnej. 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 ustawa o ochronie danych osobowych ma zastosowanie, np. ze względu na podmiot zgłaszający zbiór, czy zbiór został zgłoszony przez podmiot zobowiązany, tj. przez

administratora danych, czy zgłoszenie dotyczy jednego zbioru danych, a ponadto czy nie występują przesłanki zwolnienia z obowiązku rejestracji określone w art. 43 ust. 1 ustawy[133].

W 2014 roku wysłano do wnioskodawców **617 pism informujących o braku obowiązku rejestracji zbioru,** wynikającym z przesłanek określonych w art. 43 ust. 1 ustawy oraz **750 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.

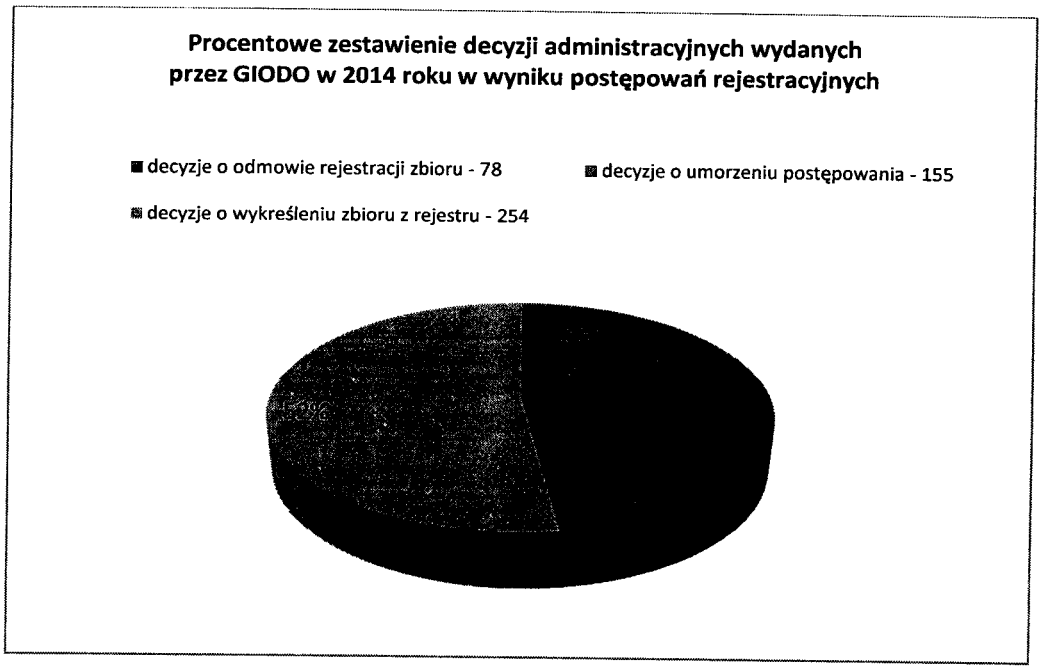
Jeżeli zgłoszenie pozytywnie przejdzie wstępną weryfikację, to w kolejnym etapie ustala się, czy nie zachodzi przesłanka odmowy rejestracji zgłoszonego zbioru danych. Zgodnie bowiem z art. 44 ust. 1 ustawy Generalny Inspektor Ochrony Danych Osobowych odmawia, w drodze decyzji administracyjnej, rejestracji 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 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

---

[133] W roku 2014 z obowiązku zgłoszenia zbioru danych osobowych do rejestracji zwolnieni byli 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.

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 **487 decyzje administracyjne w związku z postępowaniem rejestracyjnym.** Spośród nich **78 decyzje dotyczyły odmowy rejestracji zbioru danych, 155 – umorzenia postępowania, 254 decyzji dotyczyło wykreślenia** zbioru danych z ogólnokrajowego jawnego rejestru zbiorów danych osobowych.

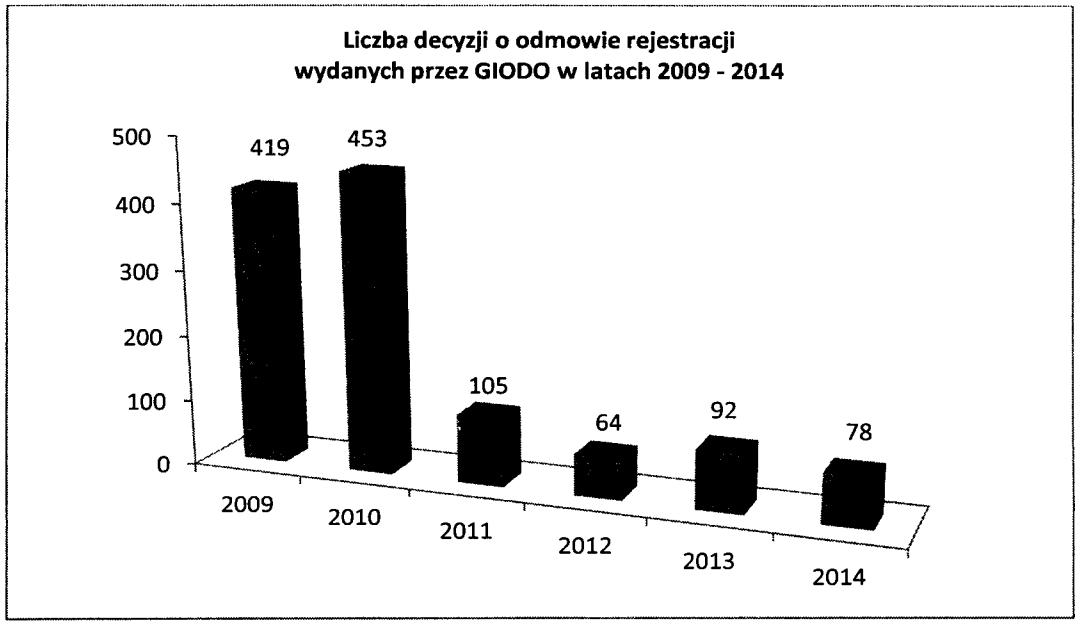


Wykres 27: ***Procentowe zestawienie decyzji administracyjnych dotyczących postępowań rejestracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2014 r.***

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **78 decyzji o odmowie rejestracji zbioru danych.**

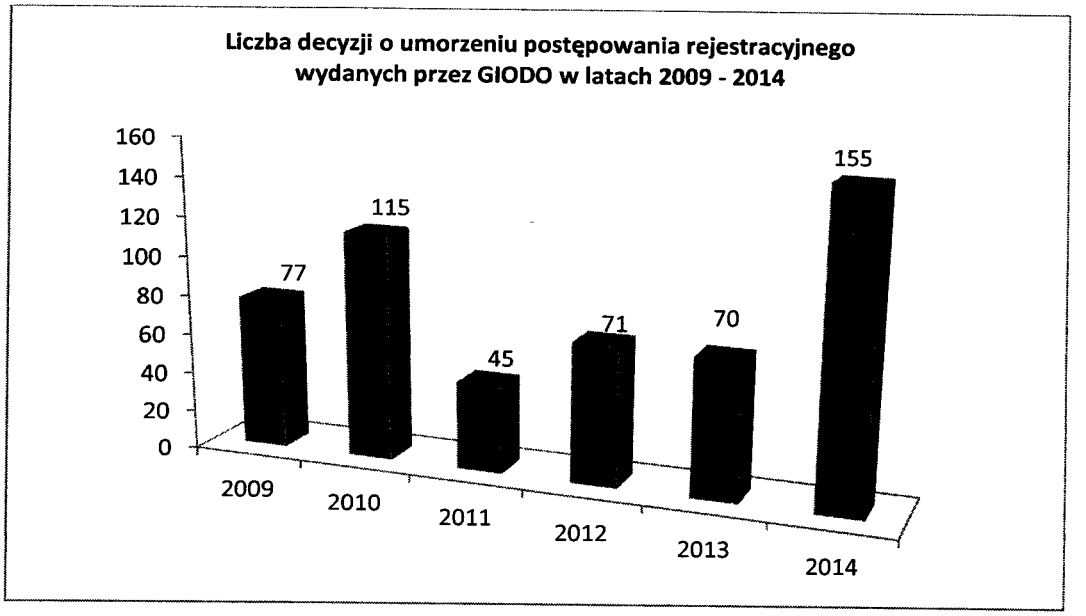
Podkreślenia wymaga fakt, że w żadnym przypadku administrator danych nie złożył wniosku o ponowne rozpatrzenie sprawy, a w konsekwencji nie było również w omawianym okresie sprawozdawczym skarg na decyzje o odmowie rejestracji do wojewódzkiego sądu administracyjnego.

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 2014 r. poz. 1619 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 Biura Generalnego Inspektora Ochrony Danych Osobowych.



Wykres 28: ***Liczbowe zestawienie decyzji o odmowie rejestracji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2012 - 2014 r.***

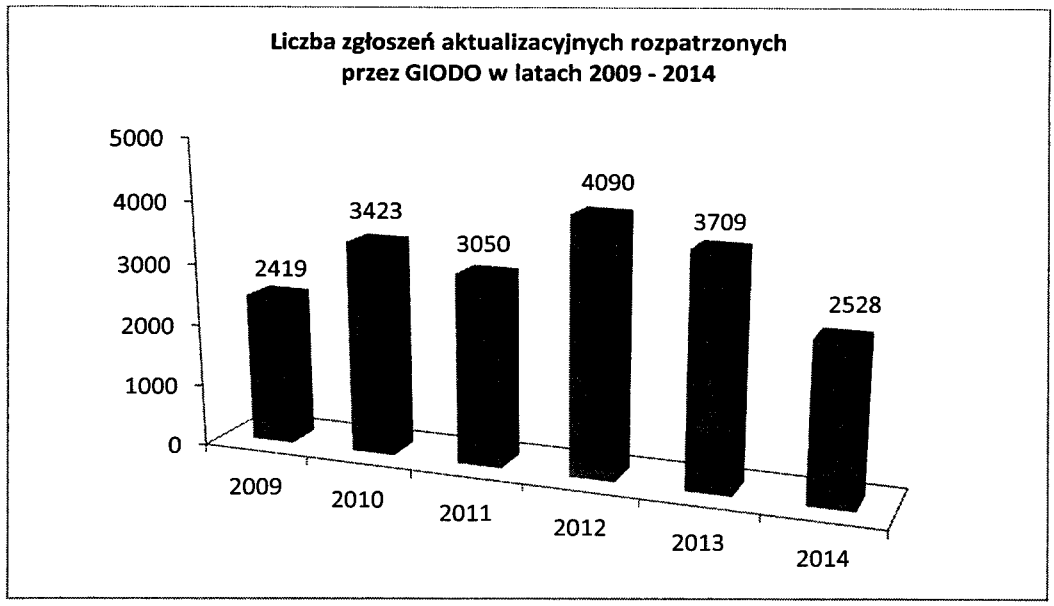
Ponadto wydanych zostało **155 decyzji o umorzeniu postępowania rejestracyjnego**, - w sytuacji gdy wnioskodawca cofa zgłoszenie, np. informując, że zrezygnował z utworzenia zbioru danych osobowych. W takich sytuacjach postępowanie rejestracyjne staje się bezprzedmiotowe i konieczne jest wydanie decyzji o jego umorzeniu.



Wykres 29: ***Zestawienie porównawcze liczby decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2014.***

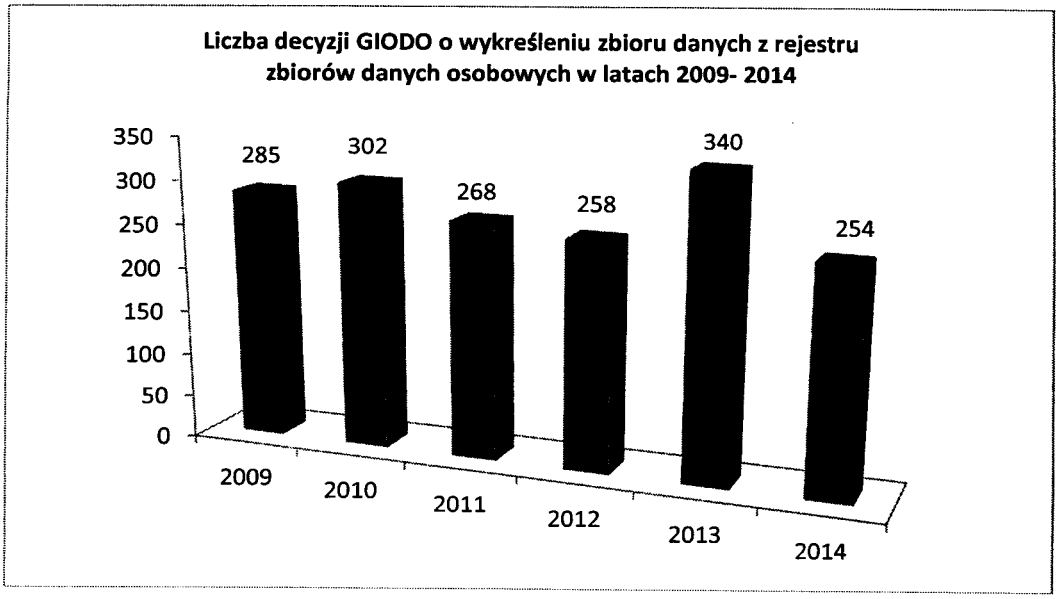
Zadania Departamentu Rejestracji Zbiorów Danych Osobowych związane z prowadzeniem rejestru zbiorów danych osobowych obejmują również rozpatrywanie zgłoszeń aktualizacyjnych, tj. zgłoszeń zmian informacji zawartych w zgłoszeniu rejestracyjnym[134] oraz prowadzenie postępowań w sprawie wykreślenia z rejestru zbiorów danych osobowych. Instytucje te dają możliwość porządkowania rejestru, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych. W 2014 roku **rozpatrzonych zostało 2528 zgłoszeń aktualizacyjnych** dokonanych przez administratorów danych na podstawie art. 42 ust. 2 ustawy.

[134] Zgodnie z art. 41 ust. 2 i 3 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 jeśli zmiana dotyczy rozszerzenia zakresu przetwarzanych danych o dane szczególnie chronione, przed dokonaniem zmiany.



Wykres 30: ***Zestawienie porównawcze liczby zgłoszeń aktualizacyjnych rozpatrzonych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008 - 2013***

Ponadto Generalny Inspektor Ochrony Danych Osobowych wydał **254 decyzje o wykreśleniu zbioru** danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych z powodu zaprzestania przetwarzania danych w zbiorze. Należy przy tym zaznaczyć, iż decyzja, o której mowa powyżej 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 2014 roku wykreślono z rejestru 446 zbiorów** danych osobowych.



Wykres 31: ***Zestawienie porównawcze liczby zbiorów wykreślonych z rejestru zbiorów danych osobowych w latach 2012 - 2014.***

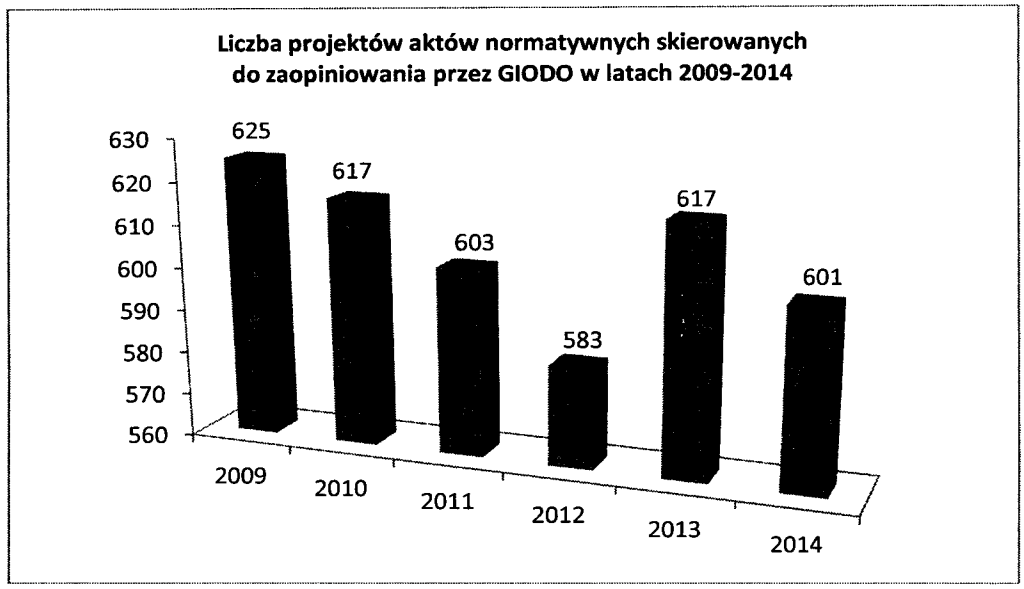
Ponadto Generalny Inspektor Ochrony Danych Osobowych wydał w omawianym okresie **2610 zaświadczeń o zarejestrowaniu zbioru danych.** W przypadku zarejestrowania zbioru danych, w którym przetwarzane są dane osobowe szczególnie chronione, określone w art. 27 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wydaje zaświadczenie z urzędu, niezwłocznie po dokonaniu rejestracji takiego zbioru[135]. Administrator danych może także wystąpić z wnioskiem do Generalnego Inspektora Ochrony Danych Osobowych o wydanie zaświadczenia o zarejestrowaniu zbioru[136].

7. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych.

Uprawnienie przyznane Generalnemu Inspektorowi przez ustawodawcę w art. 12 pkt 5 ustawy o ochronie danych osobowych pozwala na eliminowanie nieprawidłowości dotyczących przetwarzania danych osobowych już na etapie tworzenia prawa. Stosownie do treści tego przepisu, do zadań Generalnego Inspektora należy opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych.

[135] Art. 42 ust. 4 ustawy.
[136] Art. 42 ust. 3 ustawy

W roku 2014 do Biura GIODO wpłynęło do zaopiniowania **601 projektów aktów prawnych.** Jednocześnie należy zwrócić uwagę, iż 40 projektów, które poddawano analizie stanowiło kontynuację w związku z wpływem spraw w latach uprzednich (2008-2013).



Wykres 32: ***Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2008-2014.***

W 2014 roku zostały ostatecznie sfinalizowane – toczące się od 2012 roku[137] – prace legislacyjne dotyczące **ustawy z dnia 7 listopada 2014 roku o ułatwieniu wykonywania działalności gospodarczej**[138] nowelizującej ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[139]. Wprowadzone w art. 9 **ustawy o ułatwieniu wykonywania działalności gospodarczej** zmiany ustawy o ochronie danych osobowych koncentrują się na kwestiach:

1) wzmocnienia pozycji (przewidzianego już w przepisach dotychczas obowiązujących[140]) administratora bezpieczeństwa informacji;
2) uproszczenia realizacji obowiązku rejestracji zbiorów danych osobowych, o którym mowa w rozdziale 6 ustawy o ochronie danych osobowych;

[137] DOLiS-033-306/12 i DOLiS-033-450/13.
[138] Dz. U. z 2014 r. poz. 1662.
[139] Dz. U. z 2014 r. poz. 1182, z późn. zm.
[140] Art. 36 ust. 3 ustawy o ochronie danych osobowych w brzmieniu sprzed 1 stycznia 2015 r.

3) ułatwienia administratorom danych przekazania danych do tzw. państw trzecich[141] - w przypadku spełnienia określonych warunków.

Realizacji pierwszego z wymienionych wyżej celów służy z jednej strony – określeniu - w ustawie o ochronie danych osobowych wymagań minimalnych, jakie spełniać musi osoba chcąca sprawować funkcję administratora bezpieczeństwa informacji (pełna zdolność do czynności prawnych oraz korzystanie z pełni praw publicznych, niekaralność za umyślne przestępstwo, odpowiednia wiedza w zakresie ochrony danych osobowych[142]) oraz ustalenie usytuowania administratora bezpieczeństwa informacji w strukturze administracyjnej administratora danych (organizacyjna odrębność administratora bezpieczeństwa informacji i jego bezpośrednia podległość kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych[143]), z drugiej zaś – scharakteryzowaniu zadań, które realizować ma administrator bezpieczeństwa informacji (zapewnienie przestrzegania przepisów o ochronie danych osobowych u danego administratora danych, prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych[144]).

W zakresie drugiego zagadnienia ustawodawca zdecydował o zwolnieniu z obowiązku rejestracji zbiorów danych administratora danych przetwarzającego dane w zbiorze, który nie jest prowadzony z wykorzystaniem systemów informatycznych (chyba że zbiór ten zawiera dane, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych[145])[146] oraz administratora danych przetwarzającego dane „zwykłe"[147] w zbiorach prowadzonych z wykorzystaniem systemów informatycznych, jeśli administrator ten powołał administratora bezpieczeństwa informacji i zgłosił go do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[148].

Co do kwestii trzeciej – umożliwiono administratorom danych przekazanie danych osobowych do państw trzecich niezapewniających na swoim terytorium odpowiedniego poziomu ochrony danych osobowych bez zgody Generalnego Inspektora Ochrony Danych Osobowych, jeśli administratorzy ci zapewnią odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez standardowe

[141] Definicja tego pojęcia znajduje się w art. 7 pkt 7 ustawy o ochronie danych osobowych.
[142] Art. 36 a ust. 5 ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.
[143] Art. 36 a ust. 7 i 8 ustawy o ochronie danych osobowych obowiązujące od dnia 1 stycznia 2015 r.
[144] Art. 36 a ust. 2 ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.
[145] Dane sensytywne.
[146] Art. 43 ust. 1 pkt 12 ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.
[147] Nienależące do katalogu danych z art. 27 ust. 1 ustawy o ochronie danych osobowych.
[148] Art. 43 ust. 1 a ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.

klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską[149] lub prawnie wiążące reguły lub polityki ochrony danych osobowych, które zostały zatwierdzone przez Generalnego Inspektora Ochrony Danych Osobowych[150]. Wprowadzono także przepisy regulujące procedurę i zasady zatwierdzania przez Generalnego Inspektora Ochrony Danych Osobowych prawnie wiążących reguł lub polityk ochrony danych osobowych[151].

Co do pozostałych zmian ustawy o ochronie danych osobowych przewidzianych w art. 9 **ustawy o ułatwieniu wykonywania działalności gospodarczej** należy wspomnieć o: nałożeniu na Generalnego Inspektora Ochrony Danych Osobowych obowiązku prowadzenia jawnego rejestru administratorów bezpieczeństwa informacji[152] i korespondującego z nim obowiązku administratorów danych zgłaszania do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych powołania i odwołania administratora bezpieczeństwa informacji[153] (oraz zmiany informacji objętych zgłoszeniem)[154], umożliwieniu Generalnemu Inspektorowi Ochrony Danych Osobowych występowania do administratorów bezpieczeństwa informacji wpisanych do rejestru administratorów bezpieczeństwa informacji o dokonanie u administratora danych sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i przedstawienia organowi do spraw ochrony danych osobowych sprawozdania w tym zakresie[155] oraz możliwości powołania przez administratora danych zastępców administratora bezpieczeństwa informacji spełniających wymagania minimalne, o których mowa była wcześniej[156].

Stwierdzić należy, iż w czasie ponad dwuletnich prac prowadzących do ostatecznego uchwalenia **ustawy o ułatwieniu wykonywania działalności gospodarczej** Generalny Inspektor Ochrony Danych Osobowych i podlegli mu pracownicy brali udział w szeregu spotkań z podmiotami zainteresowanymi nowelizacją ustawy o ochronie danych osobowych, zaś w Biurze Generalnego Inspektora Ochrony Danych Osobowych została wytworzona znaczna ilość dokumentów (opinii, analiz, odpowiedzi do uczestników procesu legislacyjnego) mających związek z proponowanymi zmianami. Choć zatem ostateczny

[149] Zgodnie z art. 26 ust. 4 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku 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.).

[150] Art. 48 ust. 2 ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.

[151] Art. 48 ust. 3–5 ustawy o ochronie danych osobowych obowiązujące od dnia 1 stycznia 2015 r.

[152] Art. 46 c ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.

[153] Art. 46 a ust. 1–3 ustawy o ochronie danych osobowych obowiązujące od dnia 1 stycznia 2015 r.

[154] Art. 46 a ust. 5 ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.

[155] Art. 19 b ust. 1 i 2, art. 36 a ust. 2 pkt 1 lit. a i art. 36 c ustawy o ochronie danych osobowych obowiązujące od dnia 1 stycznia 2015 r.

[156] Art. 36 a ust. 6 ustawy o ochronie danych osobowych obowiązujący od dnia 1 stycznia 2015 r.

kształt **ustawy o ułatwieniu wykonywania działalności gospodarczej** stanowi kompromis między (niekiedy całkowicie sprzecznymi) oczekiwaniami osób i jednostek organizacyjnych przetwarzających dane osobowe, to przyjęte rozwiązania zostały zaakceptowane przez organ do spraw ochrony danych osobowych, zaś dla administratorów danych stanowią ważny krok umożliwiający im przygotowanie się do przyszłych zmian wprowadzanych w projektowanym rozporządzeniu unijnym dotyczącym przetwarzania danych osobowych. Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej została opublikowana w Dz. U. z 2014 r. poz. 1662.

Przedmiotem szczególnej troski Generalnego Inspektora Ochrony Danych Osobowych - w 2014 roku był projekt **ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw**[157], dotyczący m.in. problematyki informatyzacji sądów powszechnych.

Już w pierwszej opinii do projektu[158] Generalny Inspektor Ochrony Danych Osobowych stwierdził, że rozwiązania zaproponowane w tym projekcie mogą budzić wątpliwości w kontekście – statuowanej w art. 10 ust. 1 Konstytucji Rzeczypospolitej Polskiej – zasady trójpodziału władz. O ile bowiem bezspornym jest, że Minister Sprawiedliwości, jako podmiot zobowiązany do wykonywania zadań związanych z informatyzacją sądów (art. 175 b §1 ustawy z dnia 27 lipca 2001 roku – Prawo o ustroju sądów powszechnych[159], dodawany przez art. 1 pkt 40 projektu), winien posiadać takie uprawnienia, które pozwolą mu na swobodne wywiązywanie się ze spoczywających na nim w tym zakresie obowiązków, to budzić musi obiekcje przyznanie temu ministrowi statusu administratora danych w odniesieniu do danych stron, pełnomocników i innych uczestników postępowań sądowych przetwarzanych w centralnych systemach teleinformatycznych obsługujących postępowanie sądowe lub sądy (art. 175 a § 3 w zw. z § 2 ustawy – Prawo o ustroju sądów powszechnych, dodawany przez art. 1 pkt 39 projektu). W opinii organu do spraw ochrony danych osobowych zdecydowanie bardziej prawidłowym byłoby usytuowanie w projektowanych przepisach Ministra Sprawiedliwości jako administratora systemu teleinformatycznego służącego do obsługi postępowania sądowego, bez wyposażania go w możliwość władczego decydowania o celach i środkach przetwarzania danych osobowych zgromadzonych w aktach spraw sądowych (które to uprawnienie – zgodnie z art. 7 pkt 4 ustawy o ochronie danych

[157] DOLiS-033-23/14.

[158] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 18 lutego 2014 roku o sygn. DOLiS-033-23/14/TG/12661 do Podsekretarza Stanu w Ministerstwie Sprawiedliwości.

[159] Dz. U. z 2015 r. poz.133, z późn. zm.

osobowych – jest immanentnie związane ze statusem administratora danych). Generalny Inspektor Ochrony Danych Osobowych stoi na stanowisku, iż drugie z przedstawionych wyżej rozwiązań nie pozbawiłoby Ministra Sprawiedliwości realnych możliwości wykonywania zadań związanych z informatyzacją sądownictwa, a jednocześnie nie rodziłoby wątpliwości, co do wkroczenia przez organ władzy wykonawczej w – chronioną konstytucyjnie – sferę działalności niezależnego wymiaru sprawiedliwości.

Organ do spraw ochrony danych osobowych wyraził także sprzeciw wobec przyznania Ministrowi Sprawiedliwości kompetencji do przechowywania i archiwizowania akt spraw sądowych prowadzonych w całości lub w części w systemie teleinformatycznym (art. 175 b § 1 pkt 5 ustawy – Prawo o ustroju sądów powszechnych, dodawany przez art. 1 pkt 40 projektu). W jego opinii to sądy, jako organy konstytucyjnie upoważnione do sprawowania wymiaru sprawiedliwości (art. 10 ust. 2 Konstytucji Rzeczypospolitej Polskiej), winny być wyłącznie uprawnione do przetwarzania danych osobowych, w tym szczególnie chronionych, zawartych w aktach prowadzonych przez siebie postępowań, jak również decydować (zgodnie z określonymi przepisami i procedurami) o udostępnianiu danych z tych akt. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych kompetencja Ministra Sprawiedliwości (przedstawiciela władzy wykonawczej) może w tym zakresie obejmować jedynie dostarczenie sądom stosownego oprogramowania i sprzętu komputerowego umożliwiającego sprawne prowadzenie (w tym przechowywanie i archiwizowanie) akt sądowych w systemie teleinformatycznym. Organ do spraw ochrony danych osobowych zauważył również, iż w świetle obowiązujących przepisów (ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach[160]) archiwizowanie akt spraw sądowych, w tym także mających postać dokumentu elektronicznego, należy do archiwów państwowych (po upływie określonego prawem okresu przechowywania akt w poszczególnych sądach) i – w opinii Generalnego Inspektora Ochrony Danych Osobowych – nie istnieje uzasadnienie dla wprowadzenia przez projekt w tej kwestii jakichkolwiek zmian.

Podobnie wypowiadał się przeciwko zaproponowanemu w art. 1 pkt 40 projektu nowemu unormowaniu (projektowany art. 175 b § 1 pkt 4 ustawy – Prawo o ustroju sądów powszechnych), zgodnie z którym Minister Sprawiedliwości miałby dokonywać transkrypcji zapisu dźwięku z przebiegu jawnych posiedzeń sądów. Przepis taki, w przypadku jego wejścia w życie, oznaczałby w istocie dostęp Ministra Sprawiedliwości do ogromnej liczby

[160] Dz. U. z 2011 r. Nr 123, poz. 698, z późn. zm.

danych osobowych uczestników postępowań sądowych, przeciwko czemu Generalny Inspektor Ochrony Danych Osobowych oponował.

Organ do spraw ochrony danych osobowych był ponadto przeciwny – zamieszczonej w art. 12 pkt 2 projektu – propozycji utworzenia Centralnej Bazy Danych Osób Pozbawionych Wolności (nowy rozdział 4 a ustawy z dnia 6 czerwca 1997 roku – Kodeks karny wykonawczy[161]). Podnosił, że przedmiotowa regulacja jest zbyt szczątkowa, by mogła zostać zaakceptowana w świetle – określonych w art. 27 ustawy o ochronie danych osobowych zasad przetwarzania danych szczególnie chronionych. W myśl art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych – przetwarzanie takich danych bez zgody osoby, której dotyczą, wymaga przepisu szczególnego rangi ustawowej stwarzającego przy tym pełne gwarancje ich ochrony. Nie można równocześnie pominąć konieczności przestrzegania przez projektodawcę standardów wynikających z rozdziału III Konstytucji Rzeczypospolitej Polskiej dotyczących hierarchii źródeł prawa i zakresu materii, która może podlegać unormowaniu w przepisach podustawowych (wykonawczych)[162].

Tymczasem, wbrew wyżej zaprezentowanym przepisom i poglądom wyrażanym przez Trybunał Konstytucyjny, projektodawca zdecydował, że zakres informacji gromadzonych w Centralnej Bazie Danych Osób Pozbawionych Wolności (będącej bezspornie bazą danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych) ma być ustalony w rozporządzeniu (proponowany art. 25 a ust. 5 ustawy – Kodeks karny wykonawczy). Co więcej, w projekcie (za wyjątkiem nazwy własnej bazy) nie określono nawet, czyje dane osobowe mają znaleźć się w przedmiotowej bazie danych, a co za tym idzie – jakie przesłanki decydować będą o umieszczeniu (bliżej określonych jedynie w akcie wykonawczym) danych osoby w Centralnej Bazie Danych Osób Pozbawionych Wolności - oraz w jakich przypadkach (albo czy w ogóle) dane tej osoby będą z tej bazy usuwane. Wobec

[161] Dz. U. Nr 90, poz. 557, z późn. zm.

[162] Trybunał Konstytucyjny w uzasadnieniu postanowienia z dnia 31 stycznia 2007 roku (Sygn. akt S 1/2007) stwierdził, że: „Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować" funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. [...] Także art. 31 ust. 3 Konstytucji wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki. W takim wypadku zakres materii pozostawianych do unormowania w rozporządzeniu musi być węższy niż zakres materii ogólnie dozwolony na tle art. 92 ust. 1 Konstytucji. Artykuł 31 ust. 3 Konstytucji silniej bowiem akcentuje konieczność szerszego unormowania rangi ustawowej i zawęża pole regulacyjne pozostające dla rozporządzenia.".

tak istotnych braków opiniowanej regulacji zachodziła konieczność jej istotnego uzupełnienia przez projektodawcę.

W uwagach szczegółowych organ do spraw ochrony danych osobowych zgłosił też zastrzeżenia do art. 157 §1 b ustawy – Prawo o ustroju sądów powszechnych, dodawanego przez art. 1 pkt 36 lit. b projektu. W kwestionowanym przepisie, regulującym zakres informacji zamieszczanych w wykazie biegłych sądowych, projektodawca posłużył się sformułowaniem „w szczególności". Tym samym wskazany w (projektowanym) art. 157 § 1 b ustawy – Prawo o ustroju sądów powszechnych katalog danych osobowych biegłych sądowych stał się katalogiem otwartym, a co za tym idzie – w świetle proponowanego brzmienia tego przepisu, w wykazie biegłych sądowych mogłyby się znaleźć dowolne dane osobowe tych biegłych. Takie ujęcie dyspozycji komentowanego przepisu pozostaje w sprzeczności z wiążącą administratorów danych – na podstawie art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych – zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane. Dlatego też zasadnym wydaje się usunięcie z (projektowanego) art. 157 § 1 b ustawy – Prawo o ustroju sądów powszechnych sformułowania „w szczególności".

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych skutkowały wprowadzeniem przez Ministerstwo Sprawiedliwości istotnych poprawek do projektu **ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw** (wersja z dnia 28.04.2014 r.), powoływanego dalej z zastosowaniem skrótu „projekt z dnia 28.04.2014 r.".

Przedmiotem sporu między organem do spraw ochrony danych osobowych a projektodawcą pozostał art. 175 a § 3 w zw. z § 2 ustawy z dnia 27 lipca 2001 roku – Prawo o ustroju sądów powszechnych, dodawany przez art. 1 pkt 36 projektu z dnia 28.04.2014 r., zgodnie z którym Minister Sprawiedliwości ma być administratorem danych osobowych w odniesieniu do danych stron, pełnomocników uczestników postępowań sądowych i innych osób uczestniczących w postępowaniach sądowych zawartych w centralnych systemach teleinformatycznych obsługujących postępowanie sądowe lub sądy. Generalny Inspektor Ochrony Danych Osobowych konsekwentnie stał na stanowisku, że wzgląd na zasadę trójpodziału władz (art. 10 ust. 1 Konstytucji Rzeczypospolitej Polskiej) oraz zasadę odrębności i niezależności władzy sądowniczej od innych władz (art. 173 Konstytucji Rzeczypospolitej Polskiej) zdecydowanie przemawia za przyznaniem Ministrowi Sprawiedliwości w projektowanych przepisach statusu administratora systemu

teleinformatycznego służącego do obsługi postępowania sądowego, nie zaś statusu administratora danych, czyli podmiotu decydującego o celach i środkach przetwarzania danych osobowych, a zatem mogącego w sposób władczy decydować o przetwarzaniu danych osobowych zgromadzonych w aktach spraw sądowych[163]. Oprócz odwołania się i podtrzymania argumentacji podniesionej wcześniej[164], Generalny Inspektor Ochrony Danych Osobowych zwrócił także uwagę na wyrok Trybunału Konstytucyjnego z dnia 8 maja 2014 roku[165], w którym Trybunał Konstytucyjny uznał za niezgodny z Konstytucją Rzeczypospolitej Polskiej przepis rozporządzenia (§ 20 rozporządzenia Ministra Sprawiedliwości z dnia 20 grudnia 2012 roku w sprawie nadzoru administracyjnego nad działalnością administracyjną sądów powszechnych[166]) upoważniający Ministra Sprawiedliwości do żądania od prezesa sądu apelacyjnego przedstawienia mu akt spraw sądowych. Trybunał Konstytucyjny dostrzegł przy rozpoznawaniu sprawy wagę – podniesionego przez Prokuratora Generalnego – zarzutu naruszenia przez zakwestionowany przepis zasady podziału i równowagi władz oraz zasady odrębności władzy sądowniczej[167].

Zarysowany wyżej spór przeniesiony został na forum Stałego Komitetu Rady Ministrów, gdzie Generalny Inspektor Ochrony Danych Osobowych powtórzył poprzednie zarzuty, wzbogacając je o argument, że przyznanie Ministrowi Sprawiedliwości statusu administratora danych w odniesieniu do danych uczestników postępowań sądowych (w szerokim rozumieniu tego pojęcia) zawartych w centralnych systemach teleinformatycznych obsługujących postępowanie sądowe lub sądy, implikować będzie po jego stronie konieczność wypełniania, określonych w ustawie o ochronie danych osobowych, obowiązków administratora danych (np. obowiązek zapewnienia merytorycznej poprawności przetwarzanych danych[168]). Tym samym, w świetle przepisów ustawy o ochronie danych osobowych, Minister Sprawiedliwości, jako administrator danych byłby nie tylko

[163] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 13 maja 2014 roku o sygn. DOLiS-033-23/14/TG/36365 do Pana Michała Królikowskiego – ówczesnego Podsekretarza Stanu w Ministerstwie Sprawiedliwości.

[164] W piśmie o sygn. DOLiS-033-23/14/TG/12661.

[165] Sygn. akt U 9/13.

[166] Dz. U. z 2013 r. poz. 69.

[167] Komunikat po wyroku na stronie internetowej http://trybunal.gov.pl/rozprawy/komunikaty-prasowe/komunikaty-po/art/6843-upowaznienie-ministra-sprawiedliwosci-do-zadania-od-prezesa-sadu-apelacyjnego-akt-spraw-sadowy/.

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

uprawniony, ale wręcz zobowiązany do wprowadzania zmian do danych osobowych zebranych przez sądy przy rozpoznawaniu spraw[169].

Organ do spraw ochrony danych osobowych ponowił też propozycję[170], by dla realizacji – określonych w projekcie z dnia 28.04.2014 r. – zadań Ministra Sprawiedliwości związanych z informatyzacją sądownictwa, przyznać temu organowi status administratora systemu teleinformatycznego służącego do obsługi postępowania sądowego.

W następstwie ustaleń poczynionych na posiedzeniu Stałego Komitetu Rady Ministrów oraz spotkania między przedstawicielami Generalnego Inspektora Ochrony Danych Osobowych a reprezentantami Ministra Sprawiedliwości ustalono, iż uwaga organu do spraw ochrony danych osobowych w zakresie przyznania Ministrowi Sprawiedliwości statusu administratora systemu teleinformatycznego służącego do obsługi postępowania sądowego zostanie uwzględniona w ostatecznej wersji projektu **ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw**[171].

Niestety, w trakcie prac sejmowych dotyczących rządowego projektu **ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw** (druk sejmowy nr 2680) wyżej zarysowany kompromis został zerwany i Minister Sprawiedliwości został uznany za administratora danych stron, pełnomocników uczestników postępowań sądowych i innych osób uczestniczących w postępowaniach sądowych zawartych w centralnych systemach teleinformatycznych obsługujących postępowanie sądowe lub sądy oraz danych osobowych zebranych w ramach sprawowanego przez niego nadzoru zewnętrznego nad sądami oraz w związku z uprawnieniem do żądania podjęcia przez rzecznika dyscyplinarnego czynności dyscyplinarnych[172].

Prezydent Rzeczypospolitej Polskiej nie podpisał uchwalonej przez Parlament ***ustawy z dnia 20 lutego 2015 roku o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw*** zawierającej wyżej wskazane unormowania i wystąpił do Trybunału Konstytucyjnego z wnioskiem o zbadania jej zgodności z Konstytucją Rzeczypospolitej Polskiej w trybie tzw. kontroli prewencyjnej.

---

[169] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 3 czerwca 2014 roku o sygn. DOLiS-033-23/14/42581 do Pani Małgorzaty Hirszel – Sekretarz Stałego Komitetu Rady Ministrów.

[170] Z pisma o sygn. DOLiS-033-23/14/TG/12661.

[171] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 20 czerwca 2014 roku o sygn. DOLiS-033-23/14/47612 do Sekretarza Stałego Komitetu Rady Ministrów.

[172] Art. 175 a §2 i 3 ustawy – Prawo o ustroju sądów powszechnych, w brzmieniu nadanym przez art. 1 pkt 39 ***ustawy z dnia 20 lutego 2015 roku o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw***.

W roku 2014 podjęte zostały prace ustawodawcze zmierzające do odmiennego uregulowania zasad przetwarzania danych przez – utworzone na podstawie ustawy z dnia 9 kwietnia 2010 roku o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych – biura informacji gospodarczej[173], jak również umożliwienia tym biurom pozyskiwania informacji o zobowiązaniach publicznoprawnych. Trzeba wszakże zauważyć, - iż w pracach tych zabrakło koordynacji międzyresortowej, co skutkowało zamieszczeniem przepisów dotyczących powyższych kwestii w kilku projektach i to znajdujących się na różnym etapie procesu uchwalania. Na potrzeby niniejszego dokumentu wspomnieć wypada o dwóch z nich, gdyż w ich przypadku organ do spraw ochrony danych osobowych miał możliwość wypowiedzenia się już na etapie opracowywania założeń.

I tak, do dokumentu ***„Projekt założeń projektu ustawy o zmianie ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych"***[174], Generalny Inspektor Ochrony Danych Osobowych zgłosił kilka istotnych uwag.

Zamieszczona w części III pkt 1. lit. a projektu założeń propozycja projektodawcy (Ministerstwa Gospodarki), zgodnie z którą organy publiczne byłyby (po wejściu w życie projektowanych rozwiązań) uprawnione do przekazywania do biur informacji gospodarczej informacji o niektórych niespłaconych zobowiązaniach publicznoprawnych (po spełnieniu określonych dodatkowych wymagań) stanowi próbę kompromisu między – zgłaszanymi w trakcie prac nad dokumentem *„System informacji o wiarygodności płatniczej w obrocie gospodarczym. Zielona Księga"*[175] – postulatami umożliwienia przekazywania do biur informacji gospodarczej informacji o wszelkich niezapłaconych w terminie zobowiązaniach publicznoprawnych (przeciwko czemu przedstawiciel organu do spraw ochrony danych osobowych oponował na spotkaniach dotyczących dokumentu *„System informacji o wiarygodności płatniczej w obrocie gospodarczym. Zielona Księga"*), a zgłaszanymi poglądami uznającymi za niedopuszczalne przekazywanie do biur informacji gospodarczej informacji o zobowiązaniach tego rodzaju.

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych nie sprzeciwiał się, co do zasady, rozwiązaniu zaproponowanemu w części III pkt 1. lit. a projektu założeń, jednakże zgłosił swoje wątpliwości dotyczące dwóch kwestii.

---

[173] Dz. U. z 2014 r. poz. 1015, z późn. zm.

[174] DOLiS-033-173/14.

[175] Do dokumentu tego nie była sporządzana opinia pisemna; przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych uczestniczył w posiedzeniach gremium, które opracowywało ten dokument.

Po pierwsze – istnieje niezgodność między brzmieniem propozycji zawartej w części III pkt 1. lit. a projektu założeń, a uzasadnieniem tej propozycji. Tym samym z tekstu projektu założeń nie wynika jednoznacznie, czy przekazywaniu do biur informacji gospodarczej mają podlegać informacje o zaległościach (potwierdzonych ostatecznymi decyzjami administracyjnymi lub prawomocnymi wyrokami sądowymi i poddanych już egzekucji administracyjnej) z tytułu wszelkich niespłaconych podatków, czy też jedynie z tytułu niezapłaconych podatków lokalnych. Zależnie zaś od przyjętej interpretacji brzmienia części III pkt 1. lit. a projektu założeń, ilość informacji o zobowiązaniach publicznoprawnych mogących podlegać przekazaniu do biur informacji gospodarczej będzie się zasadniczo różnić, co nie pozostaje bez wpływu na stopień, w jakim proponowane unormowania będą ingerować w prawa osób, których dane mają być przekazywane.

Po drugie zaś – choć ingerencja ustawodawcy w gwarantowane konstytucyjnie prawa obywateli (do prywatności[176]; do ochrony danych osobowych[177]) jest dopuszczalna przy spełnieniu wymogu ustawowej regulacji takiego ograniczenia[178] (który to warunek jest spełniony w niniejszej sprawie), to nie może umknąć uwadze, że propozycja zamieszczona w części III pkt 1. lit. a projektu założeń stanowi istotne rozszerzenie fiskalnej roli państwa. Rozszerzenie takie nie powinno być automatycznie uznawane za sprzeczne z prawami człowieka, lecz musi podlegać testowi zgodności z regulacjami konstytucyjnymi (wymóg „konieczności ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw w demokratycznym państwie"[179], „zakaz pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym"[180]). Dopiero pozytywny wynik takiego testu, stwierdzający, iż dane wkroczenie w sferę praw i wolności obywatelskich (w tym m.in. – w prawo do prywatności i prawo do ochrony danych osobowych) jest niezbędne dla osiągnięcia społecznie oczekiwanego celu, uzasadnia interwencję legislacyjną. Dlatego o przeprowadzenie takiego właśnie testu przez projektodawcę Generalny Inspektor Ochrony Danych Osobowych wnosi.

Wzgląd na zasady przetwarzania danych osobowych (obowiązek zapewnienia przez administratora danych merytorycznej poprawności i aktualności przetwarzanych danych, zakaz przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą,

[176] Art. 47 Konstytucji Rzeczypospolitej Polskiej.
[177] Art. 51 Konstytucji Rzeczypospolitej Polskiej.
[178] Art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.
[179] Art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.
[180] Art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej.

dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania[181]) uniemożliwia organowi do spraw ochrony danych osobowych akceptację propozycji zamieszczonej w części III pkt 12 projektu założeń. Po pierwsze – w opinii Generalnego Inspektora Ochrony Danych Osobowych opiera się ona na błędnym założeniu o rzekomej niemożliwości usunięcia przetwarzanych danych[182], które to założenie w istocie podważa sens istnienia ustawy o ochronie danych osobowych. Po drugie – umożliwienie biurom informacji gospodarczej przechowywania informacji gospodarczych o zobowiązaniach wygasłych podważa samą istotę działania tych biur jako podmiotów, których przedmiotem działalności jest zbieranie informacji o zobowiązaniach niespłaconych w terminie i udostępnianie takich informacji swoim klientom[183], przy spełnieniu wymagań określonych w ustawie o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych oraz regulaminie zarządzania danymi zatwierdzonym przez ministra właściwego do spraw gospodarki. Po trzecie wreszcie – przyjęcie rozwiązania zaproponowanego w części III pkt 12 projektu założeń stworzyłoby z biur informacji gospodarczej, nieznane dotychczas polskiemu ustawodawstwu, podmioty, które raz pozyskawszy określoną informację są uprawnione do jej przechowywania w nieskończoność.

Zgodnie z Protokołem ustaleń nr 8/2015 posiedzenia Rady Ministrów w dniu 24 lutego 2015 r. (RM-000-8-15) Rada Ministrów przyjęła ***Projekt założeń projektu ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych*** postanawiając o wyłączeniu z dokumentu fragmentu odnoszącego się do pozyskiwania danych z rejestru dłużników publicznoprawnych, którego powstanie przewiduje procesowany przez Ministra Finansów projekt założeń projektu ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji.

W odniesieniu zaś do dokumentu ***„Projekt założeń projektu ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji oraz niektórych innych ustaw (ZD 101)"***[184], organ do spraw ochrony danych osobowych zajął pierwotnie znacznie bardziej krytyczne stanowisko.

Poważny niepokój Generalnego Inspektora Ochrony Danych Osobowych wzbudziła idea stworzenia publicznie dostępnego w sieci Internet rejestru zawierającego dane dłużników, gdyż rejestr taki stanowić będzie ingerencję w gwarantowaną konstytucyjnie

[181] Art. 26 ust. 1 pkt 3 i 4 w zw. z art. 32 ust. 1 ustawy o ochronie danych osobowych.
[182] Str. 23 projektu założeń.
[183] Art. 7 ust. 1 ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych.
[184] DOLiS-033-308/14.

autonomię informacyjną jednostki oraz prawo do prywatności[185]. Choć wkroczenie ustawodawcy w sferę konstytucyjnych praw obywatelskich jest dopuszczalne, to musi spełniać kryterium niezbędności („konieczności ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw w demokratycznym państwie"[186]) oraz proporcjonalności zastosowanego środka w stosunku do społecznie oczekiwanego efektu. Tymczasem – niezależnie od wymienionych na str. 2 projektu założeń – zamiarów Ministerstwa Finansów, które legły u podstaw rozwiązań zaproponowanych w tym projekcie, na plan pierwszy wysuwa się cel fiskalny projektowanych unormowań, realizowany środkami prowadzącymi do nadmiernej i nieuzasadnionej stygmatyzacji osób fizycznych. Równocześnie w projekcie założeń brak jest analizy możliwości zastosowania rozwiązań alternatywnych, godzących w prawa jednostki w mniejszym stopniu aniżeli upublicznienie w sieci Internet jej należności publicznoprawnych.

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych należy zwrócić uwagę na co najmniej pięć istotnych aspektów, które nie zostały uwzględnione przez autora projektu założeń w trakcie opracowywania tego dokumentu.

1) Informacja raz wprowadzona do Internetu ma tendencję do "klonowania się" i rozpowszechniania bez wiedzy i woli wprowadzającego. Jest również praktycznie nieusuwalna z archiwów internetowych. W sytuacji, gdy znacząca część osób prowadzących działalność gospodarczą popada w czasową zwłokę w regulowaniu swoich zobowiązań wobec Skarbu Państwa oraz Zakładu Ubezpieczeń Społecznych, oznacza to, że faktycznie większość przedsiębiorców ma szansę trafić – choćby na krótki okres czasu – do przewidzianego w projekcie założeń jawnego Rejestru Dłużników Należności Publicznoprawnych,. Informacja o tym, że ich dane umieszczone były w rejestrze będzie – mimo najlepszych procedur po stronie Ministerstwa Finansów – klonowana do innych istniejących na rynku baz informacji, takich jak informatory prawno-gospodarcze będące częścią systemów informacji prawnej, czy bazy typu „KtoKogo". Nie zapobiegnie temu również sposób organizacji bazy i obsługującego ją systemu teleinformatycznego po stronie organu prowadzącego rejestr wyznaczonego przez ministra właściwego do spraw finansów publicznych[187]. System ten może być bowiem odpytywany automatycznie

[185] Art. 51 ust. 1 i 2 oraz art. 47 Konstytucji Rzeczypospolitej Polskiej.
[186] Art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.
[187] Str. 5 projektu założeń.

przez roboty sieciowe, a ograniczenie takiej możliwości odpytywania maszynowego musiałoby wynikać z ustawy, gdyż w innym przypadku ograniczenie to łamałoby prawo do pozyskiwania jawnej formalnie informacji.

2) Chroniona w Polsce konstytucyjnie[188] wolność prasy umożliwi przepisywanie informacji z rejestru do gazet lub czasopism wraz z ich wydaniami internetowymi. O tym, że usunięcie z sieci zgromadzonej przez gazety – w tym tabloidy – informacji jest praktycznie niemożliwe, świadczą orzeczenia trybunałów europejskich w sprawach:
   a. C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Oy Satamedia[189];
   b. Węgrzynowski and Smolczewski v Polsce[190]) oraz
   c. C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González[191].

   Bardzo symptomatyczne jest tu ostatnie z wskazanych wyżej orzeczeń, które dotyczy ujawnienia w Internecie informacji o toczącym się postępowaniu egzekucyjnym należności wobec hiszpańskiego skarbu państwa. Mimo że postępowanie zakończyło się kilkanaście lat temu, przedsiębiorca do dziś boryka się z infamią wynikającą ze stałej dostępności w sieci, w tym dostępności dla wyszukiwarek internetowych, klonu starej informacji. Właśnie takie rozwiązanie Ministerstwo Finansów chce wprowadzić do polskiego systemu prawnego.
3) Informacja zawarta w rejestrze publicznym jest z zasady informacją publiczną dostępną co najmniej w trybie wnioskowym i podlegającą ponownemu przetwarzaniu na zasadach ustalonych w ustawie z dnia 6 września 2001 roku o dostępie do informacji publicznej[192].

   Stworzony przez Ministra Finansów rejestr będzie niewątpliwie rejestrem publicznym w rozumieniu ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne[193]. Będzie również rejestrem formalnie jawnym. Zagadnienie dostępności do ponownego przetwarzania informacji z jawnego rejestru zostało niedawno przetestowane przy udostępnieniu w sieciach elektronicznych ksiąg wieczystych. Twórcy projektu założeń zdają się być całkowicie

[188] Art. 14 i art. 54 Konstytucji Rzeczypospolitej Polskiej.
[189] Orzeczenie Europejskiego Trybunału Sprawiedliwości z dnia 16 grudnia 2008 r.
[190] Orzeczenie Europejskiego Trybunału Praw Człowieka z dnia 16 lipca 2013 r.
[191] Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r.
[192] Dz. U. z 2014 r. poz. 782, z późn. zm.
[193] Dz. U. z 2014 r. poz. 1114.

nieświadomi trudności, jakich doświadczył w tym zakresie Minister Sprawiedliwości zmuszony w kilka miesięcy po udostępnieniu ksiąg wieczystych w Internecie do rozpoczęcia nowelizacji serii ustaw, w tym ustawy o dostępie do informacji publicznej. Stało się tak w przypadku, gdy nie naruszano żadnej z dotychczas istniejących tajemnic. W projekcie założeń organ do spraw ochrony danych osobowych nie dostrzega żadnej refleksji dotyczącej tego zagadnienia, mimo oczywistego naruszenia zasad tajemnicy skarbowej. Za taką refleksję nie może być bowiem uznane lakoniczne stwierdzenie[194], iż do ustawy z dnia 29 sierpnia 1997 roku – Ordynacja podatkowa[195] proponuje się wprowadzić przepis, który stanowiłby, że ujawnienie informacji w Rejestrze Dłużników Należności Publicznoprawnych nie narusza przepisów o tajemnicy skarbowej.

4) Rozwiązanie zaproponowane na str. 4 projektu założeń łamie zasadę wyłączności regulacji ustawowej w sferze praw i wolności człowieka i obywatela[196]. Wbrew dyspozycji powołanego przepisu Konstytucji Rzeczypospolitej Polskiej oraz z naruszeniem standardów wynikających z rozdziału III Konstytucji Rzeczypospolitej Polskiej dotyczących hierarchii źródeł prawa, Ministerstwo Finansów zdecydowało, iż katalog należności pieniężnych podlegających ujawnieniu w rejestrze, a tym samym kwestia dane których dłużników należności publicznoprawnych w kwocie przekraczającej 500 zł zostaną podane do publicznej wiadomości w sieci Internet, ma być określony w rozporządzeniu ministra właściwego do spraw finansów publicznych, - a nie w ustawie (przypomnieć należy w tym miejscu stanowisko wyrażone przez Trybunał Konstytucyjny w uzasadnieniu postanowienia z dnia 31 stycznia 2007 roku[197]).

Nie wymaga też dowodu teza, że zagadnienie, którzy spośród ogółu dłużników należności publicznoprawnych zostaną publicznie „napiętnowani" poprzez opublikowanie ich danych osobowych w Internecie, stanowi materię o charakterze

[194] Str. 9 projektu założeń.
[195] Dz. U. z 2015 r. poz. 613.
[196] Art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.
[197] Sygn. akt S 1/2007: „Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować" funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. [...] Także art. 31 ust. 3 Konstytucji wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki. W takim wypadku zakres materii pozostawianych do unormowania w rozporządzeniu musi być węższy niż zakres materii ogólnie dozwolony na tle art. 92 ust. 1 Konstytucji. Artykuł 31 ust. 3 Konstytucji silniej bowiem akcentuje konieczność szerszego unormowania rangi ustawowej i zawęża pole regulacyjne pozostające dla rozporządzenia.".

zasadniczym, nie zaś kwestię techniczną. Tym samym nie może być przedmiotem regulacji zawartej w akcie podustawowym (wykonawczym).

5) Nie do pogodzenia z gwarantowanym konstytucyjnie[198] prawem człowieka do rozpatrzenia jego sprawy przez niezależny, bezstronny i niezawisły sąd jest też propozycja[199], by wpis danych osobowych dłużnika należności publicznoprawnych do rejestru następował po zakończeniu postępowania administracyjnego dotyczącego danej należności (przekraczającej 500 zł) i upływie 30 dni od dnia doręczenia dłużnikowi zawiadomienia o zagrożeniu wpisem do rejestru, niezależnie od zaskarżenia przez dłużnika istnienia (wysokości) tej należności do właściwego sądu. Takie rozwiązanie prowadzić będzie do nieuzasadnionej infamii (upublicznienie danych i prawdopodobne konsekwencje społeczno-ekonomiczne takiego upublicznienia) osób, które pozostają w sporze z organem administracji co do zasadności żądania zapłaty przez nich określonej kwoty, zanim o słuszności tego żądania rozstrzygnie podmiot niezależny od administracji. Dotyczyć może to w szczególności tych „dłużników", których należność publicznoprawna powstała wskutek zmiany interpretacji prawa przez organ administracji i zażądania zapłaty należności wyliczonej w oparciu o tę zmienioną interpretację za ostatnie 5 lat.

W uwagach szczegółowych organ do spraw ochrony danych osobowych zwrócił się o wyjaśnienie następującego zagadnienia. Na str. 5–6 projektu założeń przewidziano środek ochrony dłużnika należności publicznoprawnej w postaci sprzeciwu w sprawie wpisu do rejestru. Jednocześnie na str. 5 *in principio* projektu założeń zadeklarowano, iż dane osobowe dłużników należności publicznoprawnych przetwarzane na potrzeby ich ujawniania w rejestrze podlegają ochronie określonej ustawą o ochronie danych osobowych. Skoro[200] sprzeciw dłużnika należności publicznoprawnej może być wniesiony do wierzyciela w każdym czasie (aż do wykreślenia dłużnika i ciążącego nim obowiązku z rejestru), zaś uwzględnienie tego sprzeciwu w postępowaniu administracyjnym lub sądowo-administracyjnym skutkować będzie obowiązkiem wierzyciela zmiany wpisu ujawnionego w rejestrze poprzez wykreślenie z rejestru lub aktualizację informacji w nim zawartych[201], to powstaje pytanie co do stosunku projektowanych unormowań dotyczących sprzeciwu do już obowiązujących regulacji ustawy o ochronie danych osobowych, uprawniających

[198] Art. 45 ust. 1 Konstytucji Rzeczypospolitej Polskiej.
[199] Str. 4–5 projektu założeń.
[200] Str. 5 in fine projektu założeń.
[201] Str. 5–6 projektu założeń.

Generalnego Inspektora Ochrony Danych Osobowych do nakazania, w drodze decyzji administracyjnej, sprostowania przetwarzanych danych osobowych[202] albo ich usunięcia[203]. W szczególności chodzi o ustalenie, czy instytucja sprzeciwu jest *lex specialis* wobec przepisów ustawy o ochronie danych osobowych i wyłączony jest wniosek dłużnika należności publicznoprawnej ujawnionego w rejestrze do Generalnego Inspektora Ochrony Danych Osobowych o zastosowanie środków z art. 18 ustawy o ochronie danych osobowych, czy też obie konstrukcje prawne są od siebie niezależne i dłużnik należności publicznoprawnej ujawniony w rejestrze może z nich korzystać jednocześnie.

W następstwie spotkania z przedstawicielami Ministerstwa Finansów w Biurze Generalnego Inspektora Ochrony Danych Osobowych oraz udzielonych przez projektodawcę wyjaśnień pisemnych[204], organ do spraw ochrony danych osobowych zmodyfikował swoje stanowisko[205] i do nowej wersji (z dnia 23.09.2014 r.) dokumentu „***Projekt założeń projektu ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji oraz niektórych innych ustaw (ZD 101)***", przedstawił następujące uwagi.

1) Choć[206] ingerencja w gwarantowane konstytucyjnie prawa jednostki (w niniejszej sprawie – do autonomii informacyjnej[207] oraz do prywatności[208]) jest dopuszczalna przy spełnieniu przez ustawodawcę wymagań z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej[209], to w dalszym ciągu w projekcie założeń z 23.09.2014 r. niejasnym jest, czy projektodawca w należytym stopniu rozważył możliwość zastosowania rozwiązań alternatywnych, godzących w prawa jednostki w mniejszym stopniu. Zauważyć w tym miejscu wypada, iż na konieczność uwzględniania ochrony danych osobowych na etapie projektowania systemów teleinformatycznych (*privacy by design*) kładzie silny nacisk projektowane

---

[202] Art. 18 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

[203] Art. 18 ust. 1 pkt 6 ustawy o ochronie danych osobowych.

[204] Dostęp do danych zawartych w Rejestrze Dłużników Należności Publicznoprawnych będzie następować po wpisaniu przez osobę zainteresowaną określonej, znanej jej już w chwili wpisu, danej dotyczącej dłużnika należności publicznoprawnych; żaden podmiot nie będzie uprawniony do dostępu do danych zawartych w Rejestrze Dłużników Należności Publicznoprawnych na specjalnych warunkach.

[205] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 7 października 2014 roku o sygn. DOLiS-033-308/14/TG/78431 do Pani Agnieszki Królikowskiej – Podsekretarz Stanu w Ministerstwie Finansów.

[206] Jak zostało to już podniesione w piśmie Generalnego Inspektora Ochrony Danych Osobowych z dnia 12 września 2014 roku o sygn. DOLiS-033-308/14/TG/71719 do Podsekretarza Stanu w Ministerstwie Finansów.

[207] Art. 51 ust. 1 i 2 Konstytucji Rzeczypospolitej Polskiej.

[208] Art. 47 Konstytucji Rzeczypospolitej Polskiej.

[209] W tym kontekście Generalny Inspektor Ochrony Danych Osobowych przyjmuje z zadowoleniem uwzględnienie w projekcie założeń z 23.09.2014 r. jego uwagi z pkt IV. pisma o sygn. DOLiS-033-308/14/TG/71719.

rozporządzenie 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). Dlatego też – w ocenie organu do spraw ochrony danych osobowych – projekt założeń z 23.09.2014 r. winien być uzupełniony o postanowienia wykazujące niezbędność budowy centralnej bazy dłużników należności publicznoprawnych dla ochrony wartości konstytucyjnych wymienionych w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej, przy jednoczesnym uwzględnieniu stopnia oddziaływania tego rozwiązania na prawa jednostki i proporcjonalność zastosowanego środka w stosunku do społecznie oczekiwanego efektu.

2) Przy przyjęciu, że Rejestr Dłużników Należności Publicznoprawnych będzie rejestrem publicznym z dostępem do danych w nim zawartych na określonych warunkach organ do spraw ochrony danych osobowych zwraca się o wprowadzenie do projektu założeń z 23.09.2014 r. rozwiązań ograniczających możliwość maszynowego „odpytywania" Rejestru Dłużników Należności Publicznoprawnych przez roboty sieciowe automatycznie wysyłające do tego rejestru numery PESEL i numery NIP w wielkich ilościach[210]. Na wagę tego zagadnienia wskazują doświadczenia Ministra Sprawiedliwości dotyczące udostępniania ksiąg wieczystych w Internecie. System uruchomiony przez Ministra Sprawiedliwości został błyskawicznie wprost zasypany przez automatycznie generowane zapytania.
3) Rejestr Dłużników Należności Publicznoprawnych będzie niewątpliwie rejestrem publicznym w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. W opinii Generalnego Inspektora Ochrony Danych Osobowych niezbędne jest uwzględnienie w projekcie założeń z 23.09.2014 r. konsekwencji wynikających z art. 15 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, który to przepis (wraz z aktem wykonawczym wydanym na podstawie delegacji zawartej w ustępie 3 tego artykułu) kreuje obowiązek podmiotu prowadzącego rejestr publiczny zapewniania (na wniosek) podmiotowi publicznemu albo podmiotowi niebędącemu podmiotem publicznym, realizującym zadania publiczne na podstawie odrębnych przepisów

[210] W piśmie o sygn. DOLiS-033-308/14/TG/71719 wykazano, że ograniczenie możliwości odpytywania maszynowego musi wynikać wprost z ustawy napisanej w oparciu o komentowany projekt założeń.

albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji, nieodpłatnego dostępu do danych zgromadzonych w prowadzonym rejestrze.

Jak można zauważyć - dokumenty ***„Projekt założeń projektu ustawy o zmianie ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych"***[211] i ***„Projekt założeń projektu ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji oraz niektórych innych ustaw (ZD 101)"***[212] prezentowały odmienne koncepcje w kwestii upubliczniania informacji o zobowiązaniach publicznoprawnych (przekazanie tych informacji do biur informacji gospodarczej albo utworzenie Rejestru Dłużników Należności Publicznoprawnych). Do chwili sporządzania niniejszego dokumentu nie zostało rozstrzygnięte, która z tych propozycji zostanie przyjęta, gdyż prace legislacyjne w odniesieniu do obu dokumentów nie zostały ukończone.

W świetle – gwarantowanych konstytucyjnie – praw osoby fizycznej do ochrony prawnej jej życia prywatnego oraz do ochrony jej danych osobowych[213], w szczególności zaś w kontekście zasady proporcjonalności.[214], wzbudził zasadnicze zastrzeżenia organu do spraw ochrony danych osobowych projekt **ustawy o oświadczeniach o stanie majątkowym osób pełniących funkcje publiczne**[215].

O ile bowiem dotychczas obowiązujące przepisy (zarówno ustawa z dnia 21 sierpnia 1997 roku o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne[216], jak i unormowania zawarte w ustawach szczególnych) wiązały obowiązek składania oświadczeń o swoim stanie majątkowym (co stanowi istotne ograniczenia prawa do prywatności osoby zobowiązanej do złożenia takiego oświadczenia) z faktem posiadania przez osobę zobowiązaną do złożenia takiego oświadczenia określonego władztwa decyzyjnego[217] bądź z pełnieniem przez osobę zobowiązaną ważnej funkcji publicznej albo pełnieniem przez nią służby, to – przedstawiony do zaopiniowania – projekt ustawy rozszerza powyższy obowiązek na wszystkich pracowników urzędów skarbowych i izb skarbowych (także zatrudnionych na stanowiskach obsługi), wszystkich pracowników jednostek organizacyjnych Służby Celnej (niebędących funkcjonariuszami) oraz „zwykłych"

---

[211] DOLiS-033-173/14.
[212] DOLiS-033-308/14.
[213] Art. 47 i art. 51 Konstytucji Rzeczypospolitej Polskiej.
[214] Art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.
[215] DOLiS-033-265/14.
[216] Dz. U. z 2006 r. Nr 216, poz. 1584, z późn. zm.
[217] Czyli kompetencji do samodzielnego decydowania o sytuacji prawnej lub faktycznej innych podmiotów - albo chociaż istotnego wpływania na tę sytuację. Art 2 pkt 36 lit. d, g, h i pkt 63 lit. c projektu ustawy.

pracowników urzędów, do których stosuje się przepisy ustawy o służbie cywilnej lub ustawy - o pracownikach urzędów państwowych, i „zwykłych" pracowników samorządowych po przekroczeniu przez tych „zwykłych" pracowników urzędów i pracowników samorządowych określonego kryterium przychodowego[218]. Tym samym projekt **ustawy o oświadczeniach o stanie majątkowym osób pełniących funkcje publiczne** w kwestii wkroczenia w sferę prywatności osób fizycznych w sposób właściwie równorzędny traktuje osoby zajmujące kierownicze stanowiska państwowe (w rozumieniu art. 2 ustawy z dnia 31 lipca 1981 roku o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe[219] i osoby zatrudnione w organach administracji publicznej (urzędach skarbowych i izbach skarbowych, Służbie Celnej), które żadnego władztwa decyzyjnego (uprawnień decyzyjnych) nie posiadają. Rozwiązanie takie zostało uznane przez Generalnego Inspektora Ochrony Danych Osobowych za niezasadne.

Podobnie wątpliwości organu do spraw ochrony danych osobowych wywołała kwestia jawności oświadczeń majątkowych. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych zastanawiające jest dlaczego wszystkie[220] oświadczenia majątkowe mają być jawne. Nawet w świetle wyjaśnień zawartych w uzasadnieniu do projektu ustawy, zgodnie z którymi jawność oświadczeń majątkowych nawiązuje do[221] zasady dającej obywatelowi prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne, objęcie jawnością wszystkich osób wyliczonych w obszernym katalogu art. 2 projektu ustawy wydaje się nieproporcjonalne. Wątpliwości budzi bowiem cel tak dalekiej ingerencji w życie prywatne osób, które nie mają uprawnień decyzyjnych, a co za tym idzie – odpowiadają za swoje działanie w kontekście podległości wynikającej z wewnętrznej hierarchii struktury organu władzy. Zbyt daleko idącym wydaje się uznanie informacji o stanie majątku urzędników publicznych nieposiadających władztwa decyzyjnego za informację publiczną podlegającą ujawnieniu w drodze publikacji w Biuletynie Informacji Publicznej. Nieprzekonywający w tym kontekście jest cenzus majątkowy, ponieważ kryterium decydującym wynikającym z Konstytucji RP jest działalność organu, nie zaś każda informacja o procesie podejmowania decyzji, w tym informacje o osobach, które przyczyniły się do jej podjęcia – tym bardziej nie tych, które tylko z uwagi na swoje zarobki zobowiązane będą złożenia oświadczenia.

[219] Dz. U. z 2011 r. Nr 79, poz. 430, z późn. zm.
[220] Poza wyjątkami określonymi art. 10 ust. 2 i ew. ust. 3 projektu ustawy.
[221] Wyrażonej w art. 61 Konstytucji Rzeczypospolitej Polskiej.

Za niewystarczający uznano zapis art. 10 ust. 5 projektu ustawy uprawniający Radę Ministrów do doprecyzowania w drodze rozporządzenia, trybu ujawniania oświadczeń majątkowych, biorąc pod uwagę „konieczność zapewnienia sprawności przetwarzania informacji oraz potrzebę ochrony prawa do prywatności osób składających oświadczenie oraz osób trzecich będących osobami nieprowadzącymi działalności gospodarczej". To przepisy rangi ustawowej powinny określić podstawowe warunki przetwarzania danych, w tym zakresy ich przetwarzania oraz udostępniania, zaś kwestie techniczne powinny być określane w stosownym akcie wykonawczym. Ustawa powinna wskazać podmiot (administratora) odpowiedzialnego za zapewnienie, że przetwarzanie danych konieczne dla ujawnienia informacji publicznej poprzez opublikowanie oświadczeń na stronach BIP następuje na określonych zasadach. Na podstawie proponowanych przepisów wydaje się, że będzie nim podmiot uprawniony do odebrania oświadczenia, niemniej jednak warto wskazać i ten zakres jego obowiązków w sposób wyraźny.

W projekcie ustawy nie znalazły się również odniesienia do kwestii związanych z danymi osób trzecich. Wskazanym byłoby również doprecyzowanie terminu przez jaki oświadczenia będą ujawniane poprzez zamieszczenie na stronie Biuletynu Informacji Publicznej – czy będzie to miało miejsce przez cały okres retencji oświadczenia[222], a może przez okres sprawowania przez daną osobę funkcji publicznej.

Nie doprecyzowano w przepisach projektowanej ustawy[223], iż oświadczenie winno być ujawnione niezwłocznie po jego złożeniu, a w przypadku jego korekty zarówno wersja niepoprawna, jak i skorygowana, powinny być umieszczone na stronach Biuletynu Informacji Publicznej[224].

Powyższe uwagi Generalnego Inspektora Ochrony Danych Osobowych, mające silne oparcie zarówno w – powoływanych wcześniej – przepisach Konstytucji Rzeczypospolitej Polskiej, jak i unormowaniach *Konwencji o ochronie praw człowieka i podstawowych wolności*, sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2[225] przyznających każdemu prawo do poszanowania swojego życia prywatnego[226] i niedopuszczających – poza nielicznymi

---

[222] Art. 8 projektu ustawy.

[223] Zamiar taki jest wyrażony w uzasadnieniu do projektu ustawy – str. 46.

[224] Zgodnie z przepisami rozdziału 5 projektu ustawy korekta oświadczenia odbywa się poprzez złożenie nowego oświadczenia majątkowego i załączenie tego, które zostało uprzednio złożone.

[225] Dz. U. z 1993 r. Nr 61, poz. 284, z późn. zm.

[226] Art. 8 *Konwencji o ochronie praw człowieka i podstawowych wolności*, sporządzonej w Rzymie dnia 4 listopada 1950 r., zmienionej następnie Protokołami nr 3, 5 i 8 oraz uzupełnionej Protokołem nr 2.

wyjątkami – ingerencji władzy publicznej w korzystanie z tego prawa, wsparte także protestami innych uczestników procesu legislacyjnego, wywołały na tyle silny oddźwięk, że projektodawca – Ministerstwo Sprawiedliwości – zaniechał prac dotyczących projektu **ustawy o oświadczeniach o stanie majątkowym osób pełniących funkcje publiczne**.

Doniosły, choć nie tak daleko idący jak w przypadku poprzedniego projektu, efekt przyniosły uwagi Generalnego Inspektora Ochrony Danych Osobowych do dokumentu ***„Założenia do projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw"***[227].

Organ do spraw ochrony danych osobowych zanegował samą koncepcję[228] odstąpienia od ustawowego określenia zakresu danych i informacji gromadzonych w centralnej ewidencji pojazdów (CEP) i centralnej ewidencji kierowców (CEK). W opinii Generalnego Inspektora Ochrony Danych Osobowych dotychczasowe rozwiązanie, zgodnie z którym katalog danych i informacji podlegających zgromadzeniu w CEP i CEK normują odpowiednio art. 80 b ust. 1 – 1 b ustawy z dnia 20 czerwca 1997 roku – Prawo o ruchu drogowym[229] i art. 100 b ust. 1 tejże ustawy, jest rozwiązaniem prawidłowym, odpowiadającym konstytucyjnemu wymogowi z art. 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej. Podniesione zaś w projekcie założeń[230] argumenty projektodawcy za zmianą istniejącego stanu prawnego opierające się na kwestii złożoności i długotrwałości procesu legislacyjnego niezbędnego dla zmiany katalogu pozyskiwanych danych, jawią się jako nieprzekonujące. Zdaniem organu do spraw ochrony danych osobowych można wręcz zaproponować odwrócenie argumentacji projektodawcy i stwierdzić, że konieczność przeprowadzenia czasochłonnych zmian legislacyjnych, poprzedzonych stosownymi uzgodnieniami z zainteresowanymi podmiotami (w tym Generalnym Inspektorem Ochrony Danych Osobowych), ma istotne znaczenie gwarancyjne - dla osób, których dane są (lub mają być) przetwarzane w CEP i CEK, chroni bowiem przed nadmiernie częstymi i nie do końca przemyślanymi zmianami zakresu danych gromadzonych w tych ewidencjach. Co więcej – ustawowe określenie katalogu danych przetwarzanych w CEP i CEK jest zgodne z poglądami Trybunału Konstytucyjnego, który to organ konsekwentnie stoi na stanowisku, iż zasadnicza regulacja pewnych kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej, nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy

[227] DOLiS-033-247/14.
[228] Zamieszczoną na str. 3–4 projektu założeń.
[229] Dz. U. z 2012 r. poz. 1137, z późn. zm.
[230] Str. 3 i 4.

wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej[231]. Nie może wreszcie umknąć uwadze, że dotychczasowe przepisy ustawy – Prawo o ruchu drogowym odnoszące się do CEP i CEK były przez organ do spraw ochrony danych osobowych wskazywane jako wzorcowe i powoływane m.in. podczas prac legislacyjnych dotyczących innych projektów aktów prawnych. Tym samym ich zmiana w kierunku proponowanym przez projektodawcę stanowiłaby krok wstecz pod względem standardu ochrony praw osób, których dane są (lub mają być) gromadzone w przedmiotowych ewidencjach.

Generalny Inspektor Ochrony Danych Osobowych podtrzymał wcześniej prezentowane stanowisko w opinii do dokumentu ***„Założenia do projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw"*** (wersja z dnia 29.08.2014 r.) i – wobec deklaracji projektodawcy o zwróceniu się do Rady Legislacyjnej o ustosunkowanie się przez ten podmiot do zastrzeżeń zgłoszonych przez organ do spraw ochrony danych osobowych i wystąpił o przedstawienie dokumentu sporządzonego przez Radę Legislacyjną[232].

Konsekwentne stanowisko organu do spraw ochrony danych osobowych wsparte w pewnej mierze przez Radę Legislacyjną skutkowało przyjęciem przez Ministerstwo Sprawiedliwości w – opracowanym w 2015 roku na podstawie dokumentu ***„Założenia do projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw"*** – projekcie *ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw* rozwiązania, zgodnie z którym katalog danych osobowych przetwarzanych w CEP i CEK w dalszym ciągu unormowany będzie przepisami ustawowymi.

Opiniując projekt **ustawy o krwiodawstwie i krwiolecznictwie**[233] organ do spraw ochrony danych osobowych zgłosił zastrzeżenia do art. 20 ust. 8 i art. 49 ust. 7 pkt 4.

Pierwszy z wymienionych przepisów przewiduje współadministrowanie danymi przetwarzanymi w Krajowym Rejestrze Dawców Krwi przez Instytut Hematologii i Transfuzjologii z siedzibą w Warszawie i jednostki organizacyjne publicznej służby krwi w rozumieniu art. 4 pkt 2 projektu **ustawy o krwiodawstwie i krwiolecznictwie**, zwane dalej „jednostkami organizacyjnymi publicznej służby krwi". Rozwiązanie takie nie wydaje się

[231] Postanowienie Trybunału Konstytucyjnego z dnia 31 stycznia 2007 roku (Sygn. akt S 1/2007) – uzasadnienie

[232] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 8 września 2014 roku o sygn. DOLiS-033-247/14/TG/70298 do Pana Grzegorza Karpińskiego – ówczesnego podsekretarza, a obecnie Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych.

[233] DOLiS-033-318/14.

zasadne z punktu widzenia – zamieszczonej w art. 7 pkt 4 ustawy o ochronie danych osobowych – definicji administratora danych[234], gdyż rodzi potrzebę ustalenia zakresu odpowiedzialności Instytutu Hematologii i Transfuzjologii w Warszawie oraz jednostek organizacyjnych publicznej służby krwi za prawidłowość przetwarzania danych w Krajowym Rejestrze Dawców Krwi, a w razie zaistnienia naruszenia praw osób, których dane będą w tym rejestrze przetwarzane, każdorazowego rozstrzygania, działalność którego z podmiotów naruszenie to spowodowała. Co więcej – konstrukcja zaproponowana w art. 20 ust. 8 projektu **ustawy o krwiodawstwie i krwiolecznictwie** nie wydaje się zgodna z dalszymi przepisami tego projektu statuującymi zadania Instytutu Hematologii i Transfuzjologii w Warszawie oraz jednostek organizacyjnych publicznej służby krwi. Nie można bowiem pominąć, że w art. 43 ust. 1 pkt 14 projektu **ustawy o krwiodawstwie i krwiolecznictwie** prowadzenie Krajowego Rejestru Dawców Krwi zostało wskazane jako zadanie Instytutu Hematologii i Transfuzjologii w Warszawie, zaś art. 45 ust. 1 pkt 2 i 11 tegoż projektu nakłada na jednostki organizacyjne publicznej służby krwi obowiązek zawiadywania rejestrem dawców krwi oraz rejestrem niepożądanych zdarzeń i niepożądanych reakcji. Jeśli dodać do tego art. 20 ust. 10 projektu **ustawy o krwiodawstwie i krwiolecznictwie**, obligujący jednostki organizacyjne publicznej służby krwi do przekazywania drogą elektroniczną danych do Krajowego Rejestru Dawców Krwi, to wydaje się, iż – wbrew literalnemu brzmieniu art. 20 ust. 8 projektu **ustawy o krwiodawstwie i krwiolecznictwie** – administratorem danych przetwarzanych w Krajowym Rejestrze Dawców Krwi jest wyłącznie Instytut Hematologii i Transfuzjologii z siedzibą w Warszawie, zaś poszczególne jednostki organizacyjne publicznej służby krwi prowadzą własne rejestry, o których mowa w art. 20 ust. 1 oraz art. 45 ust. 1 pkt 2 i 11 projektu.

W świetle powyższych ustaleń Generalny Inspektor Ochrony Danych Osobowych uznał, że zachodzi potrzeba stosownej zmiany art. 20 ust. 8 projektu **ustawy o krwiodawstwie i krwiolecznictwie**.

Jeśli zaś chodzi o art. 49 ust. 7 pkt 4 projektu **ustawy o krwiodawstwie i krwiolecznictwie** przewidujący obligatoryjne odwołanie przez ministra właściwego do spraw zdrowia członka Krajowej Rady do Spraw Krwiodawstwa i Krwiolecznictwa w przypadku prawomocnego skazania tego członka za przestępstwo umyślne, to organ do spraw ochrony danych osobowych stwierdził, iż w projekcie tej **ustawy** brak jest przepisu materialnego

[234] Organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 ustawy o ochronie danych osobowych, decydujące o celach i środkach przetwarzania danych osobowych.

nakładającego na członka w/w Rady wymóg niekaralności za przestępstwo umyślne. Powstaje zatem wątpliwość, czy przy braku takiego przepisu materialnego[235] dopuszczalne jest uregulowanie zaproponowane w art. 49 ust. 7 pkt 4 projektu.

Uwagi Generalnego Inspektora Ochrony Danych Osobowych[236] zostały uwzględnione - w projekcie **ustawy o krwiodawstwie i krwiolecznictwie** (wersja z dnia 15.12.2015 r.)[237], jednakże na dzień sporządzenia niniejszego dokumentu prace legislacyjne dotyczące przedmiotowego projektu ustawy nie zostały ukończone (w dniu 15 kwietnia 2015 r. projekt ustawy o krwiodawstwie i krwiolecznictwie (UC 79) został rozpatrzony przez Komitet do Spraw Europejskich.

W 2014 roku Ministerstwo Zdrowia zainicjowało – wysoce istotną z punktu widzenia problematyki ochrony danych osobowych – zmianę przepisów odnoszących się do systemu informacji w ochronie zdrowia – projekt **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**[238]. Jednak już w tym miejscu nadmienić należy, iż – opracowany w oparciu o dokument *„Założenia do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw"*[239] – projekt **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw** z września 2014 roku nie obejmował swoim zakresem wszystkich zagadnień będących przedmiotem zainteresowania Generalnego Inspektora Ochrony Danych Osobowych.

Do tego projektu zgłoszone zostały następujące uwagi:

1) W dalszym ciągu[240] wątpliwości Generalnego Inspektora Ochrony Danych Osobowych budził zakres danych przetwarzanych w systemie informacji w ochronie zdrowia. Całkowicie niezrozumiałe dla organu do spraw ochrony danych osobowych było gromadzenie w rejestrze medycznym zwanym Centralnym Wykazem Usługobiorców danej o wykształceniu usługobiorcy (art. 15 ust. 2 pkt 2

---

[235] A więc nieokreśleniu w projektowanej **ustawie o krwiodawstwie i krwiolecznictwie** wymagań formalnych dla członków Krajowej Rady do Spraw Krwiodawstwa i Krwiolecznictwa.

[236] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 22 września 2014 roku o sygn. DOLiS-033-318/14/TG/73500 do Pana Cezarego Rzemka – ówczesnego Podsekretarza Stanu w Ministerstwie Zdrowia

[237] Opinia Generalnego Inspektora Ochrony Danych Osobowych do tej wersji projektu ustawy o krwiodawstwie i krwiolecznictwie została sporządzona w 2015 roku.

[238] DOLiS-033-340/14.

[239] DOLiS-033-465/13.

[240] Kwestia ta była już podnoszona przez Generalnego Inspektora Ochrony Danych Osobowych w trakcie opiniowania dokumentu *„Założenia do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw"*.

ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia[241], w brzmieniu nadanym przez art. 1 pkt 9 lit. a projektu **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**, powoływanego dalej z zastosowaniem skrótu „projekt ustawy"). W opinii Generalnego Inspektora Ochrony Danych Osobowych dana ta jest zbędna w procesie diagnostyki i leczenia, a zatem jej zamieszczanie w Centralnym Wykazie Usługobiorców stanowi naruszenie – statuowanej w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych – zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane.

2) Choć zaproponowane w art. 1 pkt 9 lit. b projektu ustawy brzmienie art. 15 ust. 5 ustawy o systemie informacji w ochronie zdrowia rozstrzyga[242] obiekcje Generalnego Inspektora Ochrony Danych Osobowych co do naruszenia przez przepisy ustawy o systemie informacji w ochronie zdrowia statusu ministra właściwego do spraw wewnętrznych jako administratora danych zbioru/rejestru PESEL, podnieść należy, iż projektowany art. 15 ust. 5 ustawy o systemie informacji w ochronie zdrowia dalej budzi zastrzeżenia organu do spraw ochrony danych osobowych. Skoro bowiem minister właściwy do spraw wewnętrznych ma nadal zapewnić bieżący dostęp do danych w zakresie: imienia (imion) i nazwiska, nazwiska rodowego, płci, obywatelstwa i daty urodzenia usługobiorcy[243], to gromadzenie tych samych danych w Centralnym Wykazie Usługobiorców[244] wydaje się zbędną redundancją danych. Co więcej – w uzasadnieniu projektu ustawy[245] projektodawca nie wskazał istotnego powodu przyjęcia takiego rozwiązania, ograniczając się do stwierdzenia, że „mogłoby być utrudnione zapewnienie dostępu w trybie bieżącym".

3) Proponowana w art. 1 pkt 11 lit. d projektu ustawy zmiana brzmienia art. 17 ustawy o systemie informacji w ochronie zdrowia skutkować będzie (w przypadku jej przyjęcia bez zmian) pominięciem w art. 17 ustawy o systemie informacji w ochronie zdrowia bardzo istotnego merytorycznie ustępu 4 tego przepisu.

---

[241] Dz. U. z 2015 r. poz. 636.

[242] Wyrażane przez organ do spraw ochrony danych osobowych na etapie opiniowania dokumentu *„Założenia do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw"*.

[243] Zgodnie z art. 15 ust. 5 pkt 2 ustawy o systemie informacji w ochronie zdrowia, w brzmieniu nadanym przez art. 1 pkt 9 lit. b projektu ustawy.

[244] Art. 15 ust. 5 pkt 1 ustawy o systemie informacji w ochronie zdrowia, w brzmieniu nadanym przez art. 1 pkt 9 lit. b projektu ustawy.

[245] Pkt 8 na str. 7.

4) Z punktu widzenia zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane, sprzeciw Generalnego Inspektora Ochrony Danych Osobowych budziło – proponowane w art. 7 pkt 8 projektu ustawy – brzmienie art. 49 ust. 3 ustawy z dnia 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[246]. W kwestionowanym przepisie, regulującym kwestię zakresu danych zamieszczanych w warstwie graficznej karty ubezpieczenia zdrowotnego, projektodawca posłużył się sformułowaniem „w szczególności" przy określeniu, jakie dane osobowe zawierać będzie warstwa graficzna tej karty. Tym samym – proponowany w art. 49 ust. 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w brzmieniu nadanym przez art. 7 pkt 8 projektu ustawy – katalog danych osobowych zamieszczanych w warstwie graficznej karty ubezpieczenia zdrowotnego stał się katalogiem otwartym, a co za tym idzie – w warstwie graficznej karty ubezpieczenia zdrowotnego mogłyby się znaleźć dowolne dane osobowe osób uprawnionych do jej posiadania. Dlatego – w opinii organu do spraw ochrony danych osobowych – zasadnym było usunięcie z w art. 49 ust. 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w brzmieniu nadanym przez art. 7 pkt 8 projektu ustawy, sformułowania „w szczególności".

Uwagi Generalnego Inspektora Ochrony Danych Osobowych[247] zostały uwzględnione - w projekcie **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw** (wersja z dnia 17.02.2015 r.), wszakże ta nowa wersja projektu ustawy została zasadniczo rozszerzona i była w 2015 roku przedmiotem dalszego opiniowania przez organ do spraw ochrony danych osobowych.

Projekt **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw** został w dniu 30 kwietnia 2015 roku skierowany pod obrady Stałego Komitetu Rady Ministrów.

Spośród projektów ustaw, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2014 roku warty odnotowania jest jeszcze projekt **ustawy o zmianie**

[246] Dz. U. z 2015 r. poz. 581.

[247] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 29 września 2014 roku o sygn. DOLiS-033-340/14/TG/76118 do Pana Piotra Warczyńskiego – Podsekretarza Stanu w Ministerstwie Zdrowia.

ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw[248], gdyż stanowi przykład rzeczowego potraktowania przez projektodawcę uwag organu do spraw ochrony danych osobowych.

Do projektu tego Generalny Inspektor Ochrony Danych Osobowych wniósł niżej przytoczone zastrzeżenia:

1) Uwzględniając, iż[249] zgoda osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych jest jedną z równorzędnych, a nie jedyną, przesłanką dopuszczalności przetwarzania takich danych, zbędny i merytorycznie nieuzasadniony jest art. 26 b ustawy z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej[250], dodawany przez art. 1 pkt 8 projektu. Ustawa o swobodzie działalności gospodarczej w sposób wyczerpujący reguluje kwestie związane ze składaniem wniosków o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, zwanej dalej „CEIDG", prowadzeniem CEIDG i udostępnianiem danych z CEIDG[251]. Tym samym – wbrew zaprezentowanemu w art. 1 pkt 8 projektu brzmieniu art. 26 b ustawy o swobodzie działalności gospodarczej – przetwarzanie danych przedsiębiorcy w ramach CEIDG odbywa się na podstawie przepisów prawa, nie zaś w oparciu o jego zgodę. Przedsiębiorca nie ma bowiem wpływu ani na zakres danych zawartych we wniosku o wpis do CEIDG[252], ani na to jakie jego dane będą udostępnione[253], nie może również uzyskać usunięcia jego danych w związku z odwołaniem zgody[254]. A zatem projektowany art. 26 b ustawy o swobodzie działalności gospodarczej w istocie wprowadzałby w błąd przedsiębiorcę tak co do przesłanki przetwarzania jego danych w ramach CEIDG, jak i rzeczywistego zakresu jego uprawnień. Dlatego organ do spraw ochrony danych osobowych wnioskował o wykreślenie z projektu tego przepisu.

---

[248] DOLiS-033-370/14.

[249] Zgodnie z art. 23 ust. 1 ustawy o ochronie danych osobowych.

[250] Dz. U. z 2015 r. poz. 584.

[251] Rozdział 3 ustawy o swobodzie działalności gospodarczej ze zmianami proponowanymi w art. 1 pkt 6–22 projektu.

[252] Co określa art. 25 ust. 1–2 ustawy o swobodzie działalności gospodarczej, w brzmieniu nadanym przez art. 1 pkt 6 lit. a – c projektu.

[253] Kwestię tę regulują art. 37 ust. 1 i 2 ustawy o swobodzie działalności gospodarczej oraz – nowo dodawany - (art. 1 pkt 22 projektu) –art. 39 a ust. 1 ustawy o swobodzie działalności gospodarczej.

[254] Art. 34 ust. 1 ustawy o swobodzie działalności gospodarczej, w brzmieniu nadanym przez art. 1 pkt 16 lit. a projektu.

2) W kontekście argumentów zamieszczonych w uzasadnieniu do projektu[255], jak również biorąc pod uwagę art. 39 a ust. 1 ustawy o swobodzie działalności gospodarczej[256], w opinii Generalnego Inspektora Ochrony Danych Osobowych zasadnym byłoby uzupełnienie dyspozycji art. 39 b ustawy o swobodzie działalności gospodarczej[257] o słowo „jawnych" po słowie „Do". Takie ujęcie projektowanego - art. 39 b ustawy o swobodzie działalności gospodarczej pozwoliłoby – w ocenie organu do spraw ochrony danych osobowych – na uniknięcie wątpliwości co do tego, które spośród danych przedsiębiorców zgromadzonych w CEIDG objęte są wyłączeniem proponowanym w tym przepisie.
3) Skoro projektodawca w art. 13 projektu wprowadzającego zmiany do ustawy z dnia 29 sierpnia 1997 roku o usługach turystycznych[258] zdecydował o rozszerzeniu wpisu do jawnego[259] rejestru organizatorów turystyki i pośredników turystycznych o numer PESEL przedsiębiorcy będącego osobą fizyczną[260], to wobec brzmienia art. 37 ust. 1 pkt 1 ustawy o swobodzie działalności gospodarczej[261] konsekwentnie winien w art. 7 ustawy o usługach turystycznych wyłączyć możliwość ujawniania tego numeru. W przeciwnym wypadku zaistnieje niezgodność między ustawą o swobodzie działalności gospodarczej a ustawą o usługach turystycznych, zaś prawo organizatorów turystyki i pośredników turystycznych będących osobami fizycznymi do ochrony ich danych osobowych będzie w sposób nieuzasadniony ograniczone.

Projektodawca – Ministerstwo Gospodarki – uznał, iż zagadnienia związane z ochroną danych osobowych należą do kompetencji Generalnego Inspektora Ochrony Danych Osobowych i w pełni przychylił się do dwóch pierwszych uwag organu do spraw ochrony danych osobowych, odstąpił zaś od koncepcji nowelizacji[262] ustawy o usługach turystycznych.

Projekt **ustawy o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw** na etapie przedkładania niniejszego dokumentu był rozpatrywany przez Stały Komitet Rady Ministrów.

---

[255] Część 4. pkt 21 – str. 22–23 uzasadnienia.
[256] Dodawany przez art. 1 pkt 22 projektu.
[257] Dodawanego przez art. 1 pkt 22 projektu.
[258] Dz. U. z 2014 r. poz. 196, z późn. zm.
[259] Art. 7 ust. 7 ustawy o usługach turystycznych.
[260] Art. 7 ust. 3 pkt 2 ustawy o usługach turystycznych, w brzmieniu nadanym przez art. 13 projektu.
[261] Art. 1 pkt 19 lit. a projektu.
[262] W projekcie ustawy o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw.

Projekt założeń do projektu ustawy o monitoringu wizyjnym[263] był konsultowany z GIODO przez Ministra Spraw Wewnętrznych. Dokument ten był już drugą w ostatnich latach próbą regulacji tego niezwykle ważnego obszaru kolizji prawa do prywatności oraz konieczności zapewniania porządku publicznego. Przede wszystkim GIODO **sprzeciwił się dopuszczeniu prowadzenia monitoringu w celu optymalizacji lub weryfikacji sposobów wykonywania powierzonych obowiązków wynikających ze stosunku pracy lub umów cywilnoprawnych oraz stosowaniu atrap kamer** jako mających wpływać na zachowania osób. Zwrócono także uwagę na potrzebę **przeglądu regulacji uprawniających określone służby i podmioty do prowadzenia obserwacji przy użyciu elektronicznych urządzeń optycznych oraz dostępu do takich nagrań** w związku z omawianym projektem. W zakresie zasad prowadzenia monitoringu we wszystkich proponowanych rodzajach przestrzeni sugerowano uzupełnienie propozycji, tak by była **zgodna z zasadami celowości, adekwatności i ograniczenia czasowego** ujętymi w art. 26 ustawy o ochronie danych osobowych oraz nie różnicowała w sposób znaczny metod informowania o objęciu monitoringiem. Organ ds. ochrony danych osobowych podkreślał także konieczność zagwarantowania praw osób obserwowanych poprzez wprowadzenie regulacji podobnych do tych ujętych w art. 32 i 33 ustawy o ochronie danych osobowych. **Przedstawiona propozycja ustanowienia GIODO jako organu nadzorującego prowadzenie monitoringu wizyjnego wymagałaby poważnego wzmocnienia finansowego i organizacyjnego Biura GIODO** oraz zmiany ustawy o ochronie danych osobowych, aby zapewnić skuteczność działań kontrolnych i obronę praw osób obserwowanych. Poparcie Generalnego Inspektora uzyskała propozycja przeprowadzania analizy potrzeb i celowości budowy systemu, jednakże powinna ona zostać rozszerzona o **ocenę wpływu na prywatność**.

Zrozumienie GIODO nie znalazła propozycja odrębnego uregulowania **innych rodzajów przestrzeni monitorowanej**, takich jak pas drogowy, obszary leśne czy kamery w pojazdach. **Sprzeciw został także wyrażony wobec swobodnego stosowania zaawansowanych technik obserwacji**, takich jak automatyczna identyfikacja wizerunków, analiza stanu emocjonalnego, kierunków poruszania się oraz analiza dźwięków, co sugerowałoby możliwość podsłuchiwania osób obserwowanych. Obecnie prowadzone są przez Ministra Spraw Wewnętrznych prace nad trzecią wersją projektu z uwagi na mnogość zgłoszonych uwag.

[263] DOLiS-033-523/13.

W zakresie uwag do **Projektu założeń projektu ustawy o zmianie ustawy – Prawo energetyczne oraz ustawy o zasadach pokrywania kosztów powstałych u wytwórców w związku z przedterminowym rozwiązaniem umów długoterminowych sprzedaży mocy i energii elektrycznej**[264] Generalny Inspektor poddawał w wątpliwość konieczność instalacji tzw. inteligentnych liczników w każdym gospodarstwie domowym, na zasadach określonych w tym projekcie, jako rozwiązań mogących mieć negatywny wpływ na prywatność przy jednoczesnym braku znaczących korzyści dla oszczędności w zakresie kosztów zużycia energii. Było to związane z brakiem precyzyjnej oceny potencjalnych strat ponoszonych przez odbiorców końcowych w przypadku niewłaściwego albo nieuprawnionego przetwarzania danych pomiarowych.

Zwracano także uwagę na mało precyzyjne określenie ról poszczególnych uczestników rynku, zakresu ich dostępu do danych pomiarowych, możliwych celów ich wykorzystania oraz okresów przechowywania danych. Postulowano także wydłużenie okresów, w których dokonywane będą odczyty do 60 minut. Poniżej tej granicy odczyty powinny odbywać się dopiero po uzyskaniu zgody odbiorcy końcowego, a wręcz na jego wyraźnie żądanie. Zbierane dane powinny być prawidłowo zabezpieczane m.in. poprzez stosowanie odpowiednich procedur zabezpieczeń, procedur postępowania w przypadku naruszenia zabezpieczeń oraz polityk prywatności kierowanych do odbiorców i ocen skutków przedsięwzięcia dla prywatności (tzw. *Privacy Impact Assessment*). Postulowano także wprowadzenie obowiązku zawiadamiania GIODO o naruszeniu danych osobowych. Co zostało przez projektodawcę przyjęte. Wnioskowano także o wprowadzenie regulacji uniemożliwiającej profilowanie odbiorców końcowych na podstawie informacji z systemu pomiarowego, które mogłoby mieć negatywne konsekwencje dla odbiorców końcowych oraz nie byłoby to niezbędne do osiągnięcia celu przetwarzania. Udało się to osiągnąć poprzez ustalanie precyzyjnej i zamkniętej listy celów, dla których dane mogą być przetwarzane. Projekt jest obecnie przedmiotem analiz w ramach Rady Ministrów.

Odnosząc się do dokumentu pt. **„Projekt założeń projektu ustawy o wspieraniu polubownych metod rozwiązywania sporów"**[265], GIODO zwrócił uwagę, iż ustalenie większości zasad prowadzenia list przez prezesów sądów okręgowych oraz Ministra Sprawiedliwości na podstawie rozporządzeń nie powinno następować w odniesieniu do podstawowych zasad prowadzenia list, które powinny być ustalone w aktach rangi ustawowej.

[264] DOLiS-033-329/14.
[265] DOLiS-033-385/14.

Zgodnie z art. 31 ust. 3 oraz 51 ust. 1 Konstytucji ograniczenie praw i wolności człowieka w postaci obowiązania do ujawniania informacji o swojej osobie może mieć miejsce jedynie na podstawie przepisu ustawy. Przeprowadzenie procesu legislacyjnego projektu ustawy pozwala także przeprowadzić odpowiedni proces konsultacji ze wszystkimi zainteresowanymi podmiotami.

Generalny Inspektor podkreślał także, iż prowadzenie centralnej listy mediatorów przez Ministra Sprawiedliwości oznacza, iż podmiot ten będzie wypełniał obowiązki administratora danych ze wszystkimi tego konsekwencjami, zgodnie z zasadami ustalonymi mocą przepisów ustawy o ochronie danych osobowych. Także zakres udostępniania danych ujętych na listach prowadzonych przez prezesów sądów okręgowych na rzecz Ministra Sprawiedliwości i ich wzajemna relacja powinna być wyraźnie określona w przepisach. Nie powinno dojść do sytuacji, w której na listę prowadzoną przez Ministra trafiać będą wszystkie informacje przetwarzane przez prezesów sądów okręgowych, na co wskazywały sformułowania propozycji – mowa była o kompilacji danych. Nie jest to konieczne w celu informowania uczestników postępowania o ich kwalifikacjach, które mogą być pomocne w polubownym zakończeniu sporu. Byłoby to zgodne z zasadą adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którą dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Wyjaśnienia wymagał także sposób zorganizowania w/w udostępniania danych pomiędzy prezesami sądów okręgowych a Ministrem Sprawiedliwości. Powinno ono odbywać się z w sposób uregulowany zgodnie z zasadami ochrony danych osobowych, tak by uniknąć nadmiernego przetwarzania danych zbędnych do celu informowania o osobach wpisanych na listy mediatorów. Projekt ustawy został skierowany pod obrady Sejmu.

Odnosząc się do projektu **ustawy o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw**[266], GIODO poddał w wątpliwość konieczność przetwarzania numeru PESEL w celu ustalenia tożsamości osoby fizycznej. Jest to administracyjny numer identyfikacyjny wykorzystywany w kontaktach obywatela z wieloma organami administracji. Jego publikowanie w związku z nałożeniem sankcji administracyjnej może powodować zmniejszenie poziomu ochrony tej danej osobowej. Wypada przypomnieć, ze numer PESEL jest ściśle powiązany z osobą fizyczną. Tytułem ilustracji tego argumentu wskazano, że

[266] DOLiS-033-168/14.

identyfikator ten nie jest podawany w Centralnej Ewidencji i Informacji o Działalności Gospodarczej w celu potwierdzenia tożsamości przedsiębiorcy będącego osobą fizyczną. Stosuje się w tym zakresie nr REGON oraz NIP. Projektodawca przyjął uwagi organu w toku procesu legislacyjnego. Projekt ustawy został rozpatrzony przez Stały Komitet Rady Ministrów.

W okresie sprawozdawczym do Biura GIODO skierowano również do zaopiniowania **rządowy projekt ustawy o charakterystyce energetycznej budynków**[267]. Wątpliwość Generalnego Inspektora budziło zawarcie wśród informacji, które mają być publicznie dostępne za pośrednictwem Biuletynu Informacji Publicznej organu prowadzącego centralny rejestr charakterystyki energetycznej budynków, danych dotyczących daty i miejsca urodzenia osoby uprawnionej, wpisanej do rejestru. Inspektor nie podzielił poglądu projektodawcy wyrażonego w uzasadnieniu do projektu (str. 18), iż część danych jest niezbędna do identyfikacji osoby uprawnionej. W opinii Inspektora podawanie tak szczegółowych danych jest zbędne i byłoby niezgodne z zasadą adekwatności. Publiczna część rejestru ma na celu informowanie zainteresowanych, iż osoba o określonym imieniu i nazwisku oraz posługująca się nadanym przez organ rejestrujący numerem wpisu posiada odpowiednie uprawnienia (zgodnie z treścią uzasadnienia projektu – s. 11 akapit 2). Szczegółowa weryfikacja danych osoby uprawnionej przez osobę, na której zlecenie przeprowadzana jest ocena efektywności energetycznej czy kontrola systemu ogrzewania lub klimatyzacji, jest możliwa przed wykonaniem tych czynności poprzez sprawdzenie danych osobowych ujętych w dokumencie tożsamości, a w razie wątpliwości poprzez przedstawienie decyzji o wpisie do odpowiedniego wykazu. Powyższy argument wzmacnia fakt, że w załącznikach nr 1 i 2 do projektu rozporządzenia w sprawie metodologii wyznaczania charakterystyki energetycznej budynku lub części budynku, sposobu sporządzania oraz wzorów świadectw charakterystyki energetycznej (dołączonego do projektu ustawy) projektodawca wskazał, iż do identyfikacji sporządzającego świadectwo energetyczne wystarczy jego imię i nazwisko oraz nr wpisu do rejestru (s. 8 i 11 projektu w/w rozporządzenia). Generalny Inspektor już w toku prac nad projektem założeń do projektu ustawy zwracał uwagę projektodawcy, że nie powinny podlegać ujawnieniu w ogólnodostępnym wykazie osób uprawnionych informacje dotyczące tych osób nie mające bezpośrednio związku ze sporządzaniem świadectw określonych w projekcie. Ustawa o

[267] DOLiS-033-219/14.

charakterystyce energetycznej budynków została opublikowana w Dz. U. z 2014 r., poz. 1200.

Odnosząc się do projektu **ustawy o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw**[268] GIODO zwrócił uwagę, iż w art. 9 ust. 3b pkt 1 ustawy z dnia 27 czerwca 1997 r. o służbie medycyny pracy (Dz. U. z 2004 r. Nr 125, poz. 1317, z późn. zm.), dodawanym przez art. 2 pkt 2 lit. b projektu ustawy, przewidziano delegację do wydania przez ministra właściwego do spraw zdrowia rozporządzenia dotyczącego sposobu prowadzenia rejestru lekarzy uprawnionych do przeprowadzania badań, o których mowa w art. 229 § 1, 2 i 5 Kodeksu pracy. Tymczasem w ustawie o służbie medycyny pracy, nawet po jej nowelizacji, nie znalazłyby się uregulowania dotyczące przedmiotowego rejestru. GIODO podkreślił, że to do projektodawcy należy ocena, czy regulacja taka w ustawie o służbie medycyny pracy jest potrzebna, czy też wystarczającymi będą – zawarte w przepisach ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2011 r. Nr 657 poz. 113, z późn. zm.) – uregulowania dotyczące prowadzenia baz danych o usługodawcach i pracownikach medycznych. GIODO wskazał jednocześnie, że w ramach projektowanej nowelizacji ustawy o służbie medycyny pracy, w ustawie tej powinny znaleźć się przepisy dotyczące ogólnych zasad prowadzenia rejestru lekarzy uprawnionych do przeprowadzania badań, o których mowa w art. 229 § 1, 2 i 5 Kodeksu pracy, w tym zakres przetwarzanych danych, okres ich przechowywania i zasady udostępniania danych z przedmiotowego rejestru. Ewentualne nowe rozporządzenie wykonawcze do ustawy o służbie medycyny pracy może bowiem jedynie dotyczyć kwestii technicznych i uszczegóławiających, nie zaś zasadniczych.

Wprowadzenie w znowelizowanej ustawie o służbie medycyny pracy szczegółowych zasad przetwarzania danych lekarzy na potrzeby prowadzenia rejestru lekarzy uprawnionych do przeprowadzania badań, o których mowa w art. 229 § 1, 2 i 5 Kodeksu pracy miało zapewnić odpowiedni – zgodny ze standardami konstytucyjnymi – poziom ochrony danych tych lekarzy oraz pozwoliłoby uniknąć nieprawidłowego przetwarzania ich danych, co może obecnie mieć miejsce w związku z obowiązującym rozporządzeniem Ministra Zdrowia i Opieki Społecznej w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy.

[268] DOLiS-033-275/14.

Projekt **ustawy o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw został skierowany pod obrady Rady Ministrów.**

Generalny Inspektor Ochrony Danych Osobowych przedstawił szereg uwag do **projektu ustawy o Karcie Dużej Rodziny**[269]. Wątpliwości organu wzbudziła między innymi procedura przyznawania Karty, w tym możliwość pozyskiwania danych niezbędnych do ustalenia prawa do posiadania Karty z innych źródeł niż dokumenty złożone przez osobę wnioskującą. Projektowane przepisy nie precyzowały z jakich zbiorów może korzystać wójt, by uzyskać dostęp do danych osobowych. Tymczasem to, do jakich celów mogą być wykorzystywane przez gminę dane zgromadzone w urzędowych zbiorach, musi być określone we właściwych przepisach prawa. Przepis ustawy o Karcie Dużej Rodziny nie może stanowić podstawy do przetwarzania danych zawartych w już istniejących zbiorach, w celach innych, niż dane te zostały zgromadzone. Zgodnie z art. 26 ust. 1 pkt 2 ustawy o ochronie danych osobowych, administrator jest obowiązany zapewnić, by dane były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych i z zachowaniem przepisów art. 23 i 25 ustawy o ochronie danych osobowych (art. 26 ust. 2). Jednocześnie przepisy szczególne, regulujące zasady przetwarzania danych przez wójta, wskazywać powinny wprost i precyzyjnie, że dane te mogą być przetwarzane także w związku z wydawaniem Karty Dużej Rodziny.

Generalny Inspektor wskazał również na potrzebę określenia zasad funkcjonowania systemu teleinformatycznego, za pomocą którego wykonywane będą czynności związane z realizacją ustawy. Wyjaśnienia wymagało zwłaszcza jakie dane będą gromadzone w tym systemie, czy będzie on miał charakter centralnej bazy danych oraz kto, na jakich zasadach i w jakim zakresie będzie mógł uzyskać do niego dostęp, a także jakie będą i jakimi względami uzasadnione okresy przetwarzania danych. Kwestie tego rodzaju muszą zostać uregulowane - na poziomie ustawowym, z uwagi na szeroki zakres danych, jakie mogą być przetwarzane w systemie teleinformatycznym, obejmujący również dane należące do kategorii szczególnie chronionych. Problematyczna w świetle powyższego była także rola ministra właściwego do spraw rodziny, bowiem analiza projektowanych przepisów nie pozwalała na precyzyjne

[269] DOLiS-033-383/14.

stwierdzenie czy ma on być administratorem danych osobowych czy administratorem systemu.

Projekt przewidywał *de facto* współadministrowanie danymi osobowymi przez wójta i ministra właściwego do spraw rodziny. Generalny Inspektor zwrócił uwagę, iż rozwiązanie takie nie wydaje się zasadne z punktu widzenia – zamieszczonej w art. 7 pkt 4 ustawy o ochronie danych osobowych – definicji administratora danych (organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 [ustawy o ochronie danych osobowych – przyp. autora], decydujące o celach i środkach przetwarzania danych osobowych), gdyż rodzi potrzebę ustalenia zakresu odpowiedzialności ministra właściwego do spraw rodziny oraz wójtów za prawidłowość przetwarzania danych w zbiorze, a w razie zaistnienia naruszenia praw osób, których dane będą w tym zbiorze przetwarzane, każdorazowego rozstrzygania, działalność którego z podmiotów to naruszenie spowodowała. Wyjaśnienia wymagało również, do jakiego zakresu danych osobowych będzie miał dostęp minister, a do jakich wójt. Podkreślono przy tym, iż ustawa o ochronie danych osobowych nie zna pojęcia współadministrowania danymi.

Ponadto osobnej i dogłębnej analizy wymagała kwestia, czy dostęp do danych osobowych przez ministra właściwego do spraw rodziny rzeczywiście jest niezbędny. W projekcie mowa była jedynie o pozyskiwaniu przez ministra za pomocą systemu teleinformatycznego danych o realizacji ustawy, które obejmują dane zbiorcze (m.in. liczba wydanych Kart, liczba rodzin wielodzietnych). Żadne przepisy nie regulowały natomiast celów, dla których dane zindywidualizowane miałyby być przetwarzane przez ministra i wskazywałyby na konieczność posiadania przez ministra dostępu do danych jednostkowych. Generalny Inspektor wskazał, iż szczególnie ze względu na fakt, że w zbiorach przetwarzane będą również dane wrażliwe, krąg podmiotów mających dostęp do danych posiadaczy Karty nie powinien być szerszy, niż jest to niezbędne ze względu na cel przetwarzania wynikający z przepisów ustawy.

Ustawa weszła w życie dnia 1 stycznia 2015 r. (ustawa z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny – Dz. U. z 2014 r. poz. 1863) – uwagi GIODO zostały częściowo uwzględnione.

Odnosząc się do **projektu ustawy o zmianie ustawy o Państwowym Ratownictwie Medycznym oraz niektórych innych ustaw**[270], GIODO zwrócił uwagę na fakt, iż przepisy

[270] DOLiS-033-321/14.

tego aktu przewidywały obowiązek dołączenia do wniosku o wpis do rejestru ratowników medycznych informacji z Krajowego Rejestru Karnego o niekaralności za przestępstwo umyślne przeciwko życiu lub zdrowiu albo dołączenia zaświadczenia wydanego przez odpowiednie władze lub organizacje państwa członkowskiego Unii Europejskiej lub Konfederacji Szwajcarskiej lub państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) lub innego państwa potwierdzające, że osoba ubiegająca się o wydanie prawa wykonywania zawodu nie została prawomocnie skazana za umyślne przestępstwo przeciwko życiu lub zdrowiu. Tymczasem, projekt ustawy nie zawierał przepisu materialnego nakładającego na osobę wykonującą zawód ratownika medycznego wymogu niekaralności za przestępstwo umyślne przeciwko życiu lub zdrowiu. O ile zrozumiałe może być, by osoba wykonująca zawód ratownika medycznego nie była karana za takie przestępstwo, o tyle konieczność dołączenia do wniosku odpowiednich dokumentów na potwierdzenie tego faktu powinna mieć wyraźną podstawę w przepisach ustawy. Tymczasem art. 10 ust. 1 opiniowanego projektu wśród warunków, jakie powinna spełniać osoba wykonująca zawód ratownika medycznego, nie wymieniał niekaralności za przestępstwo umyślne przeciwko życiu lub zdrowiu. Skazanie za takie przestępstwo nie było również wskazane jako przesłanka wygaśnięcia prawa wykonywania zawodu. Powstała zatem wątpliwość, czy przy braku odpowiedniego przepisu materialnego dopuszczalne było wymaganie dołączenia do wniosku o wpis do rejestru ratowników medycznych informacji z Krajowego Rejestru Karnego.

Ponadto projekt zawierał przepisy świadczące o tym, iż w odniesieniu do rejestru ratowników medycznych dochodzić będzie do współadministrowania danymi przez ministra właściwego do spraw zdrowia i wojewodów. Konstrukcja taka wydawała się niezgodna - definicją administratora danych według ustawy o ochronie danych osobowych i rodziła potrzebę ustalenia zakresu odpowiedzialności ministra właściwego do spraw zdrowia oraz wojewodów za prawidłowość przetwarzania danych w rejestrze ratowników medycznych, a w razie zaistnienia naruszenia praw osób, których dane będą w tym rejestrze przetwarzane, każdorazowego rozstrzygania, działalność którego z podmiotów to naruszenie spowodowała. Co więcej – zaproponowane rozwiązanie wydawało się niespójne z innymi przepisami projektu dotyczącymi zadań ministra właściwego do spraw zdrowia i wojewodów. Nie można bowiem pominąć, że w art. 10i ust. 1 projektu prowadzenie rejestru ratowników medycznych zostało wskazane jako zadanie ministra właściwego do spraw zdrowia, zaś art. 10i ust. 2 jako zadanie wojewody właściwego ze względu na zamierzone miejsce wykonywania zawodu

ratownika medycznego wskazuje dokonywanie wpisów oraz wykreśleń w rejestrze. Z uwagi na powyższe należało zauważyć, iż wojewodowie nie są podmiotami decydującymi o celach i środkach przetwarzania danych osobowych, a raczej podmiotami, które powinny zostać upoważnione do przetwarzania danych (dokonywania wpisów i wykreśleń w rejestrze) przez administratora danych, którym w tym wypadku będzie wyłącznie minister właściwy do spraw zdrowia.

W toku pierwszej konferencji uzgodnieniowej, która odbyła się w grudniu 2014 r. uwagi GIODO zostały częściowo uwzględnione[271].

W okresie sprawozdawczym do Generalnego Inspektora Ochrony Danych Osobowych wpłynął również **projektu założeń projektu ustawy o rewitalizacji**[272]. W uwagach do projektu GIODO zauważył, iż biorąc pod uwagę, że na potrzeby realizowania gminnego programu rewitalizacji dochodzić będzie do gromadzenia informacji i danych, a ustawa ma umożliwić pozyskiwanie co najmniej danych wskazanych w treści projektu założeń, konieczne jest zapewnienie, by zakres tych danych był adekwatny do celu ich przetwarzania (zgodnie z zasadą adekwatności, wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych, zatem – bez wyraźnego celu wskazanego w przepisach ustawy – nie powinno mieć miejsca pozyskiwanie danych pozwalających na identyfikację konkretnych osób. Innymi słowy, normy projektowanej ustawy przewidywać powinny zamknięte katalogi zarówno realizowanych celów, jak i niezbędnych, a przy tym proporcjonalnych do tychże celów danych.

Na dzień sporządzania niniejszego sprawozdania projekt znajdował się na etapie uzgodnień międzyresortowych.

W związku z przekazaniem do uzgodnień **rządowego projektu założeń ustawy o ponownym wykorzystaniu informacji sektora publicznego pismem z dnia 6 czerwca 2014 r.**[273] Generalny Inspektor zgłosił uwagi do tego projektu podkreślając, że w znaczącej części pokrywają się one z uwagami zgłoszonymi przez GIODO w dniu 25 lipca 2011 r. w piśmie do Pana Marszałka Sejmu Grzegorza Schetyny w związku z rozważanym wówczas rządowym projektem ustawy o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw (druk sejmowy nr 4434 poprzedniej kadencji Sejmu)

[271] Projekt ustawy znajduje się na etapie uzgodnień międzyresortowych.
[272] DOLiS-033-432/14.
[273] DOLiS-033-195/14.

transponującego do prawa polskiego dyrektywę Parlamentu Europejskiego i Rady w sprawie ponownego wykorzystywania informacji sektora publicznego[274].

Tak ówczesny projekt, jak i założenia projektu nowej ustawy były pozytywnie oceniane przez polski organ ochrony danych osobowych. GIODO podkreślił, że przedstawiony projekt założeń stanowi istotny i ważny wkład do pełnego wdrożenia do prawa polskiego zasad znowelizowanej niedawno dyrektywy Parlamentu Europejskiego i Rady w sprawie ponownego wykorzystywania informacji sektora publicznego (popularnie nazywanej „dyrektywą re-use"). Uregulowanie tych kwestii w omawianym projekcie należy uznać za słuszne i przeprowadzone w bardzo kompleksowy, nowoczesny i otwarty sposób. Stąd też sam duch ustawy, jak i zdecydowana większość proponowanych rozwiązań legislacyjnych, zasługuje na wsparcie.

Tym niemniej Generalny Inspektor pozwala sobie poddać rozwadze uczestników prac zagadnienia związane z ochroną danych osobowych przekazanych do ponownego przetwarzania w celach niekoniecznie zgodnych z pierwotnym celem ujawnienia tych danych w trybie dostępu do informacji publicznej a w szczególności te kwestie, w których przy przygotowywaniu projektu nie osiągnięto wymaganej przejrzystości i jasności.

Najbardziej istotnym zagadnieniem, jakie pojawiło się przy regulacji ustawowej zasad ponownego wykorzystania informacji publicznej jest potwierdzenie, że informacja publiczna gromadzona przez podmioty publiczne w ramach i dla celów zgodnych z konstytucyjną zasadą praworządności, będzie w przyszłości przetwarzana dla celów zupełnie innych, nad którymi organy władzy publicznej stracą kontrolę. Art. 7. Konstytucji RP stanowi wprost, że organy władzy publicznej działają na podstawie i w granicach prawa. Nie mają tym samym uprawnień do zmieniania celu przetwarzania informacji poza cele wyznaczone w przepisach prawa. Tymczasem podmioty, które na podstawie prawa do ponownego wykorzystania informacji publicznej przetwarzać będą taką informację w dowolnym komercyjnym lub niekomercyjnym celu, nie są już związane takim ograniczeniem i mogą twierdzić, że z informacją publiczną mogą czynić wszystko czego prawo wprost nie zabrania.

W związku z tym GIODO nie negując prawidłowości takiego rozwiązania i zgadzając się z bardzo otwartą wizją przyjętą przez twórców projektu ustawy o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw zwrócił uwagę, że musimy w przyszłości godzić się na to, że nasze dane osobowe w zakresie, w jakim będą stanowiły

[274] DOLiS-033-231/11.

informację publiczną, będą łączone z innymi danymi stanowiącymi informację publiczną, a nie będącymi danymi osobowymi, w celu tworzenia profilu osoby fizycznej.

GIODO potwierdził swoje przewidywanie z 2011 r., że dane z rejestrów publicznych uznawane będą powszechnie za informację publiczną, o ile jawność formalna rejestru nie została ograniczona. Należy zatem mieć świadomość, że dane osobowe z rejestrów osobowych ujawnianych w systemach teleinformatycznych dla zachowania zasad bezpieczeństwa obrotu, będą łączone przykładowo z:

1) danymi z dowolnych rejestrów publicznych, w których ujawniono obiekty przestrzenne (w rozumieniu ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej),
2) danymi dotyczącymi spraw zagospodarowania przestrzennego prezentowanymi dla celów tworzenia miejscowych planów zagospodarowania przestrzennego,
3) danymi z Centralnej Ewidencji i Informacji o Działalności Gospodarczej,
4) danymi z krajowych rejestrów urzędowych w rozumieniu przepisów o statystyce publicznej (REGON, TERYT),
5) publicznie dostępnymi danymi z ofert przygotowanych na podstawie przepisów o handlu wierzytelnościami,
6) oświadczeniami majątkowymi składanymi przez urzędników publicznych i członków władz publicznych oraz
7) pozostającymi w gestii danego podmiotu danymi przetwarzanymi z zachowaniem odpowiednich podstaw prawnych a dotyczących jego klientów lub potencjalnych klientów.

Informacja publiczna będzie tym samym wykorzystywana – z użyciem nowej podstawy prawnej formułowanej w prawie do ponownego wykorzystania informacji publicznej – do tworzenia profilu osobowego osoby fizycznej, czyli „automatycznej techniki przetwarzania danych polegającej na przypisaniu danej osobie 'profilu' w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji zachowań i postaw"[275]. Co więcej takie profile będą miały zarówno charakter tzw. „profili predykcyjnych" (tworzonych w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności poprzez uzupełnianie informacji publicznej o monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które

[275] Opinia Grupy art. 29 nr 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta dnia 22 czerwca 2010 r., pkt 2.3, str. 8.

klika), jak i tzw. „profili jawnych" (tworzonych na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą)[276].

W tej sytuacji Generalny Inspektor Ochrony Danych Osobowych, kontrolując działania podmiotów (komercyjnych i niekomercyjnych) polegające na tworzeniu profili przy wykorzystaniu ponownie przetwarzanej informacji publicznej, będzie ściśle stosował się do wytycznych zawartych w Rekomendacji CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich Rady Europy w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili[277].

Rada Europy podkreśliła, że technologie informacyjne i komunikacyjne pozwalają na zbieranie na wielką skalę danych, w tym danych osobowych, zarówno w sektorze publicznym jak i prywatnym. Są one wykorzystywane dla wielu celów, w tym do świadczenia usług powszechnie akceptowanych i cenionych przez społeczeństwo, konsumentów i gospodarkę. Jednocześnie szczególną uwagę organy ochrony praw człowieka powinny zwrócić na uzupełnianie informacji publicznej zawierającej dane osobowe zbierane w różnych sytuacjach i dla różnych celów: dane dotyczące ruchu, zapytania internautów, nawyki konsumenckie, dane o aktywności, stylu życia i zachowaniu użytkowników urządzeń telekomunikacyjnych, w tym dane geolokalizacyjne oraz dane pochodzące w szczególności z portali społecznościowych, systemów wideonadzoru, systemów biometrycznych oraz systemów identyfikacji za pomocą fal radiowych (RFID), „smart meteringu" i „Internetu przedmiotów". Tworzenie profili może być bowiem prowadzone w uprawnionym interesie zarówno podmiotu wykorzystującego ponownie informację publiczną, jak i osoby, której są przypisywane, na przykład jeśli stosuje się je dla poprawy segmentacji rynku, analizy ryzyka, wykrywania oszustw czy dostosowywania oferty świadczonych usług do popytu, oraz że z tego względu może ono przynieść korzyści użytkownikom, gospodarce i całemu społeczeństwu. Jednocześnie takie działanie może narazić osobę fizyczną na szczególnie wysokie ryzyko dyskryminacji i ataków na ich prawa osobiste i godność a tworzenie profili dzieci może mieć dla nich poważne konsekwencje przez całe ich życie, a nie są one zdolne samodzielnie udzielić dobrowolnej, świadomej i wyraźnej zgody na zebranie ich danych osobowych dla celów profilowania.

---

[276] Tamże

[277] Rekomendacja przyjęta przez Komitet Ministrów Rady Europy w dniu 23 listopada 2010 r. podczas 1099. posiedzenia Wiceministrów *https://wcd.coe.int/wcd/ViewDoc.jsp?id=1710949&Site=CM.*

Pożądane jest tym samym monitorowanie stosowania zasad ponownego wykorzystania informacji publicznej w zakresie, w jakim obejmuje ona dane osobowe (bądź dane, które po powiązaniu z danymi posiadanymi przez ponownie wykorzystującego stają się danymi osobowymi) w odniesieniu do ochrony danych osobowych, które pozwoli na ochronę podstawowych praw i wolności obywateli, w szczególności prawa do prywatności oraz do zapobiegania dyskryminacji ze względu na płeć, pochodzenie etniczne i rasowe, wyznanie i przekonania, niepełnosprawność, wiek czy orientację seksualną. Z punktu widzenia organu ochrony danych osobowych oznacza to m.in. że:

1) każda osoba powinna być informowana, że jej dane osobowe uzyskane przy korzystaniu z prawa do informacji publicznej są ponownie wykorzystywane na zasadach określonych w omawianej ustawie,
2) każdej osobie winno przysługiwać prawo dostępu do jej danych,
3) każda osoba powinna znać zasady kierujące danym sposobem ponownego wykorzystania informacji publicznej.

Należy jednak pamiętać, że ochrona godności ludzkiej i innych podstawowych praw i wolności, w odniesieniu do profilowania, może być skuteczna tylko i wyłącznie, jeśli wszystkie zainteresowane strony współpracują podczas tworzenia profili osób w sposób rzetelny i zgodny z prawem. Należy promować mechanizmy samoregulacji, takie jak kodeksy postępowania zapewniające poszanowanie danych osobowych i prywatności oraz do wdrażania technologii opisanych w wyżej wymienionej rekomendacji.

Osoby, których dane dotyczą, winny mieć możliwość, w zależności od potrzeb, bezpiecznego poprawiania, usuwania lub blokowania swoich danych osobowych w przypadku, gdy profilowanie związane z przetwarzaniem danych osobowych wykonywane jest niezgodnie z przepisami prawa.

W związku z tym Generalny Inspektor wnioskował o uzupełnienie projektu o odpowiednie regulacje chroniące prawo do prywatności po przekazaniu informacji publicznej do ponownego wykorzystania, w szczególności poprzez podkreślenie, że podmiot, który przejmuje informację publiczną obejmującą dane osobowe, chcąc ją wykorzystać dla celów innych niż te dla których była pierwotnie zbierana, musi wypełnić wszystkie wymagania wynikające z przepisów ustawy o ochronie danych osobowych w szczególności wymagania określone w art. 35 tej ustawy.

W grudniu 2014 r., podczas drugiego etapu uzgodnień projektu założeń do ustawy o ponownym wykorzystaniu informacji publicznej, GIODO konsekwentnie wnioskował o

uzupełnienie projektu o odpowiednie regulacje chroniące prawo do prywatności po przekazaniu informacji publicznej do ponownego wykorzystania, w szczególności poprzez podkreślenie, że podmiot, który przejmuje informację publiczną obejmującą dane osobowe, chcąc ją wykorzystać dla celów innych niż te, dla których była pierwotnie zbierana, musi wypełnić wymagania wynikające z przepisów ustawy o ochronie danych osobowych. Podkreślał, że dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. zmieniona dyrektywą Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego w sposób wyraźny stanowi, że dyrektywa powinna być wykonywana i stosowana w pełnej zgodności z regułami odnoszącymi się do ochrony danych osobowych zgodnie z dyrektywą 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 (preambuła, motyw 21). Zgodnie z art. 1 ust. 4 dyrektywy niniejsza dyrektywa pozostawia nienaruszony i w żaden sposób nie wpływa na poziom ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych zgodnie z przepisami Unii i prawa krajowego, w szczególności nie zmienia zobowiązań i praw określonych w dyrektywie 95/46/WE.

Organ do spraw ochrony danych osobowych wskazał, że określenie zasad ponownego wykorzystania w odrębnej regulacji stanowi wyjątkową i poważną szansę do stworzenia gwarancji w zakresie praw i wolności jednostki, że ponowne wykorzystanie informacji publicznej, obejmującej dane osobowe będzie następować z poszanowaniem prawa do prywatności i zasad ochrony danych osobowych.

Z dotychczasowych doświadczeń Generalnego Inspektora wynika, że istnieje realna obawa, że w świadomości podmiotów ponownie wykorzystujących informację publiczną, w szczególności podmiotów prywatnych, może pokutować przekonanie, że dopełnienie obowiązku informacyjnego nie jest konieczne w sytuacji, gdy określone informacje zostały pozyskane jako informacje publiczne. Stąd potrzebne jest zaakcentowanie odpowiedzialności podmiotów ponownie wykorzystujących informację publiczną za poszanowanie prawa do informacji osoby fizycznej i prawa do poprawiania, usuwania lub blokowania swoich danych osobowych, w przypadku, gdy przetwarzanie następuje niezgodnie z przepisami prawa.

Zgodnie z projektem założeń ustawy o ponownym wykorzystywaniu informacji sektora publicznego **z dnia 27 stycznia 2015 r.** wzorem art. 1 ust. 4 udip w brzmieniu nadanym dyrektywą 2013/37/UE wprowadzony zostanie przepis, **zgodnie z którym projektowane**

przepisy pozostają bez uszczerbku dla przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 i 1662). Ponadto prawo do ponownego wykorzystywania informacji sektora publicznego zostanie ograniczone: a) ze względu na ochronę informacji niejawnych oraz ochronę innych tajemnic ustawowo chronionych; b) ze względu na prywatność osoby fizycznej i tajemnicę przedsiębiorcy; c) informacje sektora publicznego, do których dostęp jest ograniczony na podstawie innych ustaw szczególnych[278].

Na etapie przygotowywania niniejszego sprawozdania projekt był przedmiotem prac Rady Ministrów.

W sierpniu 2014 r.[279] Generalny Inspektor Ochrony Danych Osobowych zgłosił uwagi do projektu ustawy – **Prawo o aktach stanu cywilnego**, wskazując, że art. 52 projektu uprawniał i zarazem zobowiązywał podmioty wykonujące działalność leczniczą (którymi - zgodnie z art. 2 pkt 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej – t.j. Dz. U. z 2013 r. poz. 217 z pózn. zm. – są podmioty lecznicze, o którym mowa w art. 4 tej ustawy, oraz lekarze lub pielęgniarki i położne wykonujące zawód w ramach działalności leczniczej jako praktykę zawodową), do pozyskiwania następujących danych: miejsce zamieszkania rodziców dziecka, w tym okres przebywania na terytorium Rzeczypospolitej Polskiej na obszarze danej gminy, o ile są znane, wykształcenie rodziców dziecka, informacje o stanie zdrowia dziecka: długość, ciężar ciała, punkty w skali Apgar oraz informacje o ciąży i porodzie: okres trwania ciąży i wielorakość oraz dane o poprzednich ciążach i porodach matki dziecka. Powyższe dane - zgodnie z projektowanym ustępem 3 tego artykułu podmiot wykonujący działalność leczniczą ma przekazywać służbom statystyki publicznej dla celów statystyki publicznej.

Pewne wątpliwości budziło samo umiejscowienie tego przepisu jako dotyczącego statystyki publicznej w ustawie prawo o aktach stanu cywilnego. Ustawa prawo o aktach stanu cywilnego dotychczas nie obejmowała takiego obowiązku. Powyższe wątpliwości są tym większe, że przyjęcie takiego rozwiązania nie zostało wyjaśnione przez projektodawcę w uzasadnieniu projektu. W uzasadnieniu wyjaśniono jedynie, że przekazywanie danych statystycznych wynikających z ustawy – Prawo o aktach stanu cywilnego i ustawy o

[278] Ograniczenia, o których mowa w lit. b) i c) – wzorem art. 5 ust. 2 udip – nie będą dotyczyć informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

[279] DOLiS-033-269/14.

cmentarzach i chowaniu zmarłych między podmiotami prowadzącymi działalność leczniczą a Głównym Urzędem Statystyki Publicznej mają umożliwić zmiany zaproponowane w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (art. 122 projektu ustawy) i że przekazywanie to następować będzie za pośrednictwem Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych.

W odniesieniu do art. 72 ust. 1 projektu GIODO zgłosił pytanie, dlaczego projektodawca zrezygnował z rozwiązania legislacyjnego obowiązującego obecnie, a polegającego na wyraźnym wyartykułowaniu w przepisie, że jeżeli dla przysposobionego sporządza się nowy akt urodzenia, dotychczasowego aktu nie ujawnia się. Podnieść należy, że obecnie obowiązujący art. 48 ust 3 ustawy Prawo o aktach stanu cywilnego ustawy z dnia 29 września 1986 r. Prawo o aktach stanu cywilnego (t.j. Dz. U. z 2011 r. Nr 212 poz. 1264, z późn. zm.) przewiduje taki zakaz w sposób wyraźny. Jakkolwiek w ocenie organu ochrony danych osobowych nie ulega wątpliwości, że intencją proponowanego brzmienia przepisu, jest osiągnięcie celu w postaci nieujawniania dotychczasowego aktu urodzenia, niemniej jednak powstaje pytanie o powód rezygnacji z wyraźnego zakazu w tym zakresie. W ocenie organu ochrony danych osobowych umieszczenie na tym akcie jedynie wzmianki dodatkowej odnosi się jedynie do formy wykonania obowiązku „nieujawniania" aktu i w praktyce może okazać się niewystarczające. Za wpisaniem takiego zakazu przemawia ponadto zdaniem Generalnego Inspektora Ochrony Danych Osobowych zasada jednoznaczności aktów prawnych oraz potrzeba precyzyjnego określenia zasad dostępności do informacji zawartych w księgach stanu cywilnego przez osoby zainteresowane w przypadku sporządzania nowego aktu stanu cywilnego. Akta stanu cywilnego zawierają z natury rzeczy informacje dotyczące więcej niż jednego podmiotu – w wielu przypadkach pojawia się skrzyżowanie „sfer poufności" obejmujących różne podmioty, stąd w zakresie omawianego obowiązku wskazana jest szczególna ostrożność i precyzyjność zapisu.

Analogiczne uwagi GIODO odniósł do przepisu art. 66 ust. 4 projektu, wobec którego rozważyć należało, czy nie powinien on być uzupełniony o wyraźne wskazanie, że w przypadku sporządzenia nowego aktu urodzenia lub aktu zgonu, dotychczasowego aktu urodzenia lub aktu zgonu nie ujawnia się. Jednocześnie należy wyrazić dużą aprobatę dla wprowadzenia przez projektodawcę rozwiązań postulowanych m.in. w wyroku Trybunału Konstytucyjnego z dnia 12 listopada 2002 r. SK 40/01 odnoszących się do ograniczenia ujawniania danych zawartych w zupełnych odpisach aktu stanu cywilnego związanych z ustaleniem pochodzenia dziecka.

Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (Dz. U. z 2014 r. poz. 1741), która weszła w życie 1 marca 2015 r. uwzględnia w większości uwagi Generalnego Inspektora. W zakresie postulowanym przez GIODO przepisy dotyczące sporządzania nowego aktu stanu cywilnego uzupełniono o wyraźne wyartykułowanie zakazu ujawniania dotychczasowego aktu stanu cywilnego.

W zakresie **projektu ustawy – Prawo restrukturyzacyjne**[280] zastrzeżenie wzbudził brak ujęcia szczegółowych regulacji dotyczących Centralnego Rejestru Restrukturyzacji i Upadłości.

Zauważono, iż założenia projektu ustawy- Prawo restrukturyzacyjne, stanowiły o „projektowanym utworzeniu centralnej platformy internetowej - Centralnego Rejestru Upadłości (CRU) (...). Kosztowne i wydłużające postępowanie zamieszczanie obwieszczeń - w Monitorze Sądowym i Gospodarczym oraz dzienniku o zasięgu lokalnym zostanie zastąpione ogłoszeniem w CRU."

Koniecznym uznano pilne określenie zasad prowadzenia Centralnego Rejestru Restrukturyzacji i Upadłości zwłaszcza, iż od zamieszczania w nim określonych w projekcie informacji zależeć będzie zarówno wywodzenie określonych skutków prawnych dla określonych projektem postępowań, i będą za jego pomocą przetwarzane także tzw. dane szczególnie chronione, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych.

Uwagi GIODO zostały uwzględnione. Ustawa Prawo restrukturyzacyjne została uchwalona na 92. posiedzeniu Sejmu w dniu 15 maja 2015 r.

W październiku 2014 r. Generalny Inspektor Ochrony Danych Osobowych wyraził aprobatę podejmowanych przez Ministerstwo Pracy i Polityki Społecznej prac nad **„Projektem założeń projektu ustawy o przetwarzaniu danych osobowych gromadzonych w rejestrach publicznych służb zatrudnienia (pzs)"**[281]. Zwrócił jednak uwagę, iż proponowana przez projektodawcę koncepcja wprowadzania do ustawy o ochronie danych osobowych regulacja zwalniająca rejestry pzs z obowiązku rejestracji zbioru danych osobowych w GIODO budzi wątpliwości z punktu widzenia zaproponowanego rozwiązania. Abstrahując bowiem od merytorycznej niepoprawności powyższej propozycji (zgodnie z art. 43 ust. 1 ustawy o ochronie danych osobowych, z obowiązku rejestracji zbioru danych może być zwolniony administrator danych, nie zaś jakikolwiek rejestr), sama idea wpisania do

[280] DOLiS-033-182/14.
[281] DOLiS-033-241/14.

ustawy o ochronie danych osobowych całościowego zwolnienia zbiorów danych prowadzonych przez publiczne służby zatrudnienia z obowiązku rejestracji, o którym mowa w rozdziale 6 ustawy o ochronie danych osobowych, nie wydaje się słuszna. Do dnia sporządzenia niniejszego dokumentu Ministerstwo Pracy i Polityki Społecznej nie ustosunkowało się do uwag organu do spraw ochrony danych osobowych.

Wśród projektów rozporządzeń przedstawionych organowi do spraw ochrony danych osobowych celem zaopiniowania wyróżnić należy projekt **rozporządzenia Ministra Spraw Wewnętrznych w sprawie prowadzenia Rejestru Dowodów Osobistych**[282] i projekt **rozporządzenia Rady Ministrów w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów**[283].

W pierwszym z wymienionych wyżej projektów rozporządzeń zasadnicze zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych wzbudził § 3 ust. 2 pkt 3 in fine, gdyż odczytywany literalnie kreował kompetencję Agencji Bezpieczeństwa Wewnętrznego do realizacji obowiązków administratora danych osobowych zgromadzonych w Rejestrze Dowodów Osobistych. Takie ujęcie dyspozycji § 3 ust. 2 pkt 3 in fine projektu **rozporządzenia Ministra Spraw Wewnętrznych w sprawie prowadzenia Rejestru Dowodów Osobistych** pozostawało zaś w całkowitej sprzeczności z art. 55 ust. 1 ustawy z dnia 6 sierpnia 2010 roku o dowodach osobistych[284], czyli aktem prawnym wyższej rzędu aniżeli projektowane rozporządzenie. Zgodnie bowiem z art. 55 ust. 1 ustawy o dowodach osobistych Rejestr Dowodów Osobistych prowadzi minister właściwy do spraw wewnętrznych.

Co więcej – krytykowany przepis projektu **rozporządzenia Ministra Spraw Wewnętrznych w sprawie prowadzenia Rejestru Dowodów Osobistych** pozostawał też niezgodny z art. 35 ust. 4 ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu[285], który to przepis przewiduje prowadzenie przez Agencję Bezpieczeństwa Wewnętrznego centralnego rejestru wydanych dokumentów uniemożliwiających ustalenie danych identyfikujących funkcjonariuszy i pracowników organów, służb lub instytucji prowadzących czynności operacyjno-rozpoznawcze oraz osób udzielających im pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych, jednakże odrębnego od Rejestru Dowodów Osobistych.

---

[282] DOLiS-033-287/14.
[283] DOLiS-033-354/14.
[284] Dz. U. Nr 167, poz. 1131, z późn. zm.
[285] Dz. U. z 2010 r. Nr 29, poz. 154, z późn. zm.

Wobec wykazania tak istotnych niezgodności przepisu projektu **rozporządzenia Ministra Spraw Wewnętrznych w sprawie prowadzenia Rejestru Dowodów Osobistych** - z regulacjami ustawowymi organ do spraw ochrony danych osobowych wnosił o usunięcie z § 3 ust. 2 pkt 3 projektu sformułowania: „oraz realizację obowiązków administratora danych osobowych zgromadzonych w RDO".

Ustosunkowując się do uwag Generalnego Inspektora Ochrony Danych Osobowych[286] Ministerstwo Spraw Wewnętrznych przedstawiło propozycję nowego brzmienia § 3 ust. 2 pkt 3 projektu **rozporządzenia Ministra Spraw Wewnętrznych w sprawie prowadzenia Rejestru Dowodów Osobistych**, którą organ do spraw ochrony danych osobowych zaakceptował[287].

Projekt **rozporządzenia Ministra Spraw Wewnętrznych w sprawie prowadzenia Rejestru Dowodów Osobistych** został ostatecznie zaakceptowany przez Ministra Spraw Wewnętrznych i – pod tytułem – *rozporządzenie Ministra Spraw Wewnętrznych z dnia 20 listopada 2014 roku w sprawie prowadzenia Rejestru Dowodów Osobistych* opublikowany w Dzienniku Ustaw[288]. Rozporządzenie to obowiązuje od dnia 1 marca 2015 roku.

W odniesieniu zaś do projektu **rozporządzenia Rady Ministrów w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów** wątpliwości organu do spraw ochrony danych osobowych wywołał – określony w załączniku nr 5 do tego projektu – wzór karty daktyloskopijnej odcisków linii papilarnych palców. W ocenie Generalnego Inspektora Ochrony Danych Osobowych brak jest bowiem jakiegokolwiek uzasadnienia dla zamieszczania w karcie daktyloskopijnej odcisków linii papilarnych palców informacji o narodowości osoby daktyloskopowanej i tym samym – gromadzenia takiej danej. Dana ta jest całkowicie zbędna dla celów ewentualnego postępowania karnego (art. 213 i art. 214 w zw. z art. 297 § 1 pkt 3 ustawy z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego[289] oraz art. 332 § 1 ustawy – Kodeks postępowania karnego) albo postępowania w sprawach o wykroczenia (art. 213 § 1 ustawy – Kodeks postępowania karnego w zw. z art. 54 § 8 ustawy z dnia 24 sierpnia 2001 roku – Kodeks postępowania w sprawach o

---

[286] Dokument *„Zestawienie uwag do projektu rozporządzenia MSW w sprawie prowadzenia Rejestru Dowodów Osobistych (uzgodnienia międzyresortowe)"*.

[287] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 16 września 2014 roku o sygn. DOLiS-033-287/14/TG/71929 do Pana Grzegorza Karpińskiego – ówczesnego podsekretarza, a następnie Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych.

[288] Dz. U. z 2014 r. poz. 1709, z późn. zm.

[289] Dz. U. Nr 89, poz. 555, z późn. zm.

wykroczenia[290] oraz art. 57 § 2–4 ustawy – Kodeks postępowania w sprawach o wykroczenia), jak również dla celów dowodowych, wykrywczych i identyfikacyjnych, gdyż kształt linii papilarnych jest cechą indywidualną każdego człowieka i nie jest uzależniony od jego narodowości. Co za tym idzie – zamieszczanie w karcie daktyloskopijnej odcisków linii papilarnych palców informacji o narodowości osoby daktyloskopowanej stanowi naruszenie zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane[291], i to w odniesieniu do danej będącej daną szczególnie chronioną w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych[292].

Tym samym zaproponowany w załączniku nr 5 do projektu **rozporządzenia Rady Ministrów w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów** wzór karty daktyloskopijnej odcisków linii papilarnych palców nie mógł być – w zakresie informacji o narodowości osoby daktyloskopowanej – zaakceptowany przez GIODO.

Niestety, projektodawca – Ministerstwo Spraw Wewnętrznych – nie odniósł się do zarzutów organu do spraw ochrony danych osobowych, a od października 2014 roku nie kontynuuje prac legislacyjnych dotyczących zakwestionowanego przez Generalnego Inspektora Ochrony Danych Osobowych projektu rozporządzenia.

Generalny Inspektor Ochrony Danych Osobowych brał również udział w opiniowaniu **projektu rozporządzenia Ministra Infrastruktury i Rozwoju zmieniającego rozporządzenie w sprawie wyłączenia zastosowania niektórych przepisów ustawy - Prawo lotnicze do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków**[293]. Generalny Inspektor zwrócił uwagę, iż przy pomocy bezzałogowych statków powietrznych może dochodzić do przetwarzania danych wizualnych i dźwiękowych (które, po spełnieniu określonych warunków, można traktować jako dane osobowe). Zaniepokojenie wzbudził szeroko określony zakres zastosowania bezzałogowych statków powietrznych, a mianowicie „cele inne niż rekreacyjne lub sportowe". W uzasadnieniu do projektu rozporządzenia wskazano jedynie, że tego rodzaju statkami powietrznymi realizowane są różnego rodzaju prace lotnicze (usługi). Nie uregulowano również kwestii dopuszczalności i warunków używania bezzałogowych statków powietrznych wyposażonych w urządzenia rejestrujące obraz lub

[290] Dz. U. z 2013 r. poz. 395, z późn. zm.
[291] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.
[292] Narodowość jest stanem świadomości każdego człowieka i wynikającą z tego stanu jego identyfikacją z daną grupą etniczną, dana ta wprost ujawnia pochodzenie etniczne, a niekiedy także rasowe człowieka.
[293] DOLiS-033-449/14.

dźwięk. Jak zostało wskazane w uzasadnieniu do projektu, spektrum zastosowań bezzałogowych statków powietrznych jest bardzo szerokie i zróżnicowane – obejmuje m.in. takie usługi jak fotografowanie czy filmowanie, patrolowanie granic, dróg i autostrad, koordynacja i wsparcie akcji ratunkowych. Jak również słusznie zauważono w uzasadnieniu, z lotnictwem bezzałogowym wiążą się nowe wyzwania dotyczące ochrony i poszanowania praw obywateli.

Mając na uwadze powyższe Generalny Inspektor stwierdził, iż uregulowanie zawarte w projekcie wydaje się nieostre, co stwarza pole do potencjalnych nadużyć. Jest to tym bardziej niepokojące ze względu na fakt, iż regulacja ta może potencjalnie dotykać praw obywateli, w szczególności prawa do prywatności. W opinii organu do spraw ochrony danych osobowych, wobec wielu potencjalnych możliwości zastosowania bezzałogowych statków powietrznych, należało wyraźnie sprecyzować cele, do jakich miałyby być wykorzystywane. Jeżeli natomiast przy ich użyciu miałoby dochodzić do rejestrowania dźwięku lub obrazu, a tym samym przetwarzania danych osobowych, konieczne byłoby precyzyjne uregulowanie zasad i celów ich przetwarzania w odpowiednich przepisach.

Generalny Inspektor stwierdził, iż wskazane byłoby szczegółowe określenie w odpowiednich przepisach warunków wykorzystywania bezzałogowych statków powietrznych wyposażonych w urządzenia rejestrujące obraz lub dźwięk do celów innych niż rekreacyjne lub sportowe, w szczególności poprzez:

1) wyraźne wskazanie celów, do jakich mogą być wykorzystywane tego typu statki powietrzne,
2) wskazanie na podstawie jakich przepisów miałaby następować rejestracja dźwięku lub obrazu, a tym samym przetwarzanie danych osobowych,
3) wskazanie czasu przechowywania i kręgu podmiotów mających dostęp do nagrań wykonanych za pomocą urządzeń rejestrujących.

Podkreślono również, iż z uwagi na potencjalny wpływ na prawa i wolności obywateli, regulacja tego rodzaju kwestii nie powinna następować na poziomie rozporządzenia. Do dnia sporządzenia niniejszego sprawozdania projektodawca nie ustosunkował się do uwag Generalnego Inspektora Ochrony Danych Osobowych, ani nie podjął dalszych prac nad **projektem rozporządzenia zmieniającego rozporządzenie w sprawie wyłączenia zastosowania niektórych przepisów ustawy - Prawo lotnicze do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków.**

Generalny Inspektor zgłosił również uwagi do **projektu rozporządzenia Ministra Zdrowia w sprawie orzekania o potrzebie udzielania nauczycielowi akademickiemu urlopu dla poratowania zdrowia**[294]. Wątpliwości wzbudziło umieszczenie osobnej rubryki „Uzasadnienie" we wzorze orzeczenia lekarskiego o potrzebie udzielenia nauczycielowi akademickiemu urlopu dla poratowania zdrowia.

GIODO wskazał, iż należy zastanowić się nad zasadnością wpisywania do orzeczenia szczegółowych informacji dotyczących stanu zdrowia nauczyciela, szczególnie biorąc pod uwagę fakt, iż jeden z egzemplarzy dokumentu otrzymuje także rektor uczelni. Dane o stanie zdrowia, zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych należą do kategorii danych szczególnie chronionych, zatem ich przetwarzanie jest dopuszczalne wyłącznie po spełnieniu jednego ze wskazanych w art. 27 ust. 2 ustawy warunków. W obecnie obowiązującym stanie prawnym nie ma podstaw do tego, by przekazywać pracodawcy szczegółowe dane dotyczące stanu zdrowia pracownika – pracodawca nie może bowiem żądać od pracownika podania danych innych niż wymienione w art. 22^1 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21 poz. 94 z późn. zm.), chyba że informacje te są niezbędne w celu skorzystania przez pracownika ze szczególnych uprawnień prawa pracy albo obowiązek podania informacji wynika z przepisów odrębnych ustaw. Nie wydaje się, by do skorzystania z urlopu dla poratowania zdrowia konieczne były informacje szersze, niż stwierdzenie, że ze względu na stan zdrowia nauczyciela wymagane jest udzielenie mu takiego urlopu. Ma to znaczenie zwłaszcza wobec faktu, iż projekt rozporządzenia nie precyzował również, jaki zakres informacji może znaleźć się w uzasadnieniu, ani czy rubryka ta wypełniana jest wyłącznie w przypadku, gdy stan zdrowia nauczyciela wymaga udzielenia urlopu dla poratowania zdrowia.

Generalny Inspektor wskazał ponadto, iż w analogicznej regulacji dotyczącej nauczycieli niebędących nauczycielami akademickimi, tj. rozporządzeniu Ministra Zdrowia z dnia 27 października 2005 r. w sprawie orzekania o potrzebie udzielenia nauczycielowi urlopu dla poratowania zdrowia (Dz. U. z 2005 r. Nr 233, poz. 1991), wzór orzeczenia lekarskiego (załącznik nr 1) nie zawiera osobnej rubryki przeznaczonej na uzasadnienie. Tego rodzaju wyodrębnionej części nie zawierają również wzory zaświadczeń lekarskich załączone do rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r. w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej

[294] DOLiS-033-334/14.

nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy (Dz. U. z 1996 r. Nr 69, poz. 332 z późn. zm.).

Uwaga GIODO została uwzględniona w opublikowanym rozporządzeniu Ministra Zdrowia z dnia 3 października 2014 r. w sprawie orzekania o potrzebie udzielenia nauczycielowi akademickiemu urlopu dla poratowania zdrowia (Dz. U. z 2014 r. poz. 1359).

Po przeanalizowaniu projektu **rozporządzenia Ministra Infrastruktury i Rozwoju w sprawie dokumentów oraz informacji, jakie jest obowiązany przedstawić przedsiębiorca ubiegający się o koncesję lub wykonujący działalność gospodarczą w zakresie przewozu lotniczego**[295] – zastrzeżenia GIODO wzbudziły:

1) postanowienie § 3 pkt 1 lit. b, w jakim w przypadku przedsiębiorców - osób fizycznych, nakłada na te podmioty obowiązek dołączenia do wniosku o udzielenie koncesji na podjęcie i wykonywanie działalności gospodarczej w zakresie przewozu lotniczego „kopii dokumentu potwierdzającego tożsamość, ze wskazaniem numeru PESEL i miejsca zamieszkania". Zauważono, iż ani art. 166 ust. 2 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (t.j. Dz. U. z 2013 r. poz. 1393), ani Rozporządzenie Parlamentu Europejskiego i Rady (WE) NR 1008/2008 z dnia 24 września 2008 r. w sprawie wspólnych zasad wykonywania przewozów lotniczych na terenie Wspólnoty (tekst pierwotny: Dz. Urz. UE L.2008.293.3) nie stanowi o takim obowiązku. Ponadto obowiązek podania miejsca zamieszkania w przedmiotowej sprawie istnieje jedynie wtedy, gdy działalność gospodarcza wykonywana jest pod tym adresem (adres siedziby jest tożsamy z adresem zamieszkania), nie zaś w każdym przypadku,
2) postanowienia § 3 pkt 2 lit. a tiret 1-3, które wydawały się dotyczyć spełnienia wymogów finansowych zgodnie z art. 5 rozporządzenia nr 1008/2008 przez przedsiębiorcę ubiegającego się o koncesję, nie zaś spełnienie wymogu dobrej reputacji przez członków zarządu i prokurentów,
3) postanowienie § 3 pkt 2 lit. a tiret 4, bowiem wątpliwym było, czy nałożenie obowiązku przedstawienia informacji o niekaralności z Krajowego Rejestru Karnego stanowi dopełnienie obowiązku, o którym mowa w art. 7 ust. 1 rozporządzenia nr 1008/2008. Winien tu mieć zastosowanie art. 7 ust. 2 rozporządzenia nr 1008/2008, tj. może być zastosowany wymóg złożenia

[295] DOLiS-033-492/14.

oświadczenia, o którym mowa w tym przepisie. Zauważono także, iż dane z Krajowego Rejestru Karnego stanowią tzw. dane szczególnie chronione, których przetwarzanie – stosownie do art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych – jest dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych, natomiast (co najmniej) art. 166 ustawy Prawo lotnicze takiego przyzwolenia nie daje,

4) postanowienia § 3 pkt 2 lit. b, w zakresie „w przypadku osób nieposiadających (...) nie wydaje takich dokumentów" – z przyczyn tożsamych jak w uwadze w punkcie 3), z zastrzeżeniem, iż o ile organ wydający koncesje przyjmuje jako wystarczający dowód wobec obywateli państw członkowskich przedstawienie dokumentów potwierdzających spełnienie wymogów dobrej reputacji, wydanych przez właściwe organy w państwie członkowskim pochodzenia lub w państwie członkowskim, w którym dane osoby mają swoje stałe miejsce pobytu, należy złożyć ww. dokumenty – stosownie do art. 7 ust. 1 rozporządzenia nr 1008/2008,
5) postanowienia Załączników nr 1 i 2 do projektowanego rozporządzenia, w zakresie, w jakim nie przewidują opcjonalności podania przez podmioty ubiegające się o udzielenie koncesji numeru telefonu, numeru faksu i adresu e-mail.

Pomocniczo wskazano także, iż kopie dokumentów, czy informacje, o których była mowa w § 3 pkt 1 lit. b i § 3 pkt 2 lit. a tiret 1-4, stanowią raczej dokumenty i informacje, jakie mogą być przedstawiane w trybie art. 166 ust. 4 ustawy Prawo lotnicze Prezesowi Urzędu Lotnictwa Cywilnego, gdy uzna on w toku stosownego postępowania, iż dodatkowe dane i dokumenty mogą uprawdopodobnić, że podmiot wnioskujący spełnia warunki wykonywania działalności gospodarczej, które będą określone w koncesji lub wynikają z właściwych przepisów[296].

W **projekcie rozporządzenia Ministra Infrastruktury i Rozwoju zmieniającego rozporządzenie w sprawie egzaminów dla ekspertów do spraw bezpieczeństwa przewozu towarów niebezpiecznych statkami żeglugi śródlądowej**[297] zastrzeżenia wzbudziły:

1) postanowienie § 1 pkt 1, w jakim nadano nowe brzmienie § 2 rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 6 września 2012 r. w sprawie egzaminów dla ekspertów do spraw bezpieczeństwa przewozu towarów niebezpiecznych statkami żeglugi śródlądowej (Dz. U. poz. 1045) w zakresie pkt 3,

[296] Projekt miał być skierowany pod obrady konferencji uzgodnieniowej.
[297] DOLiS-033-488/14.

stanowiącym o złożeniu wniosku o dopuszczenie do egzaminu wraz z (pkt 3) kserokopią dokumentu stwierdzającego tożsamość.

Za wątpliwe uznano istnienie konieczności przechowywania w aktach dotyczących egzaminu na „eksperta ADN" kserokopii dokumentu stwierdzającego tożsamość. Dla potwierdzenia tożsamości osoby przystępującej do egzaminu wystarczającym jest okazanie dokumentu, katalog zaś danych osobowych „ekspertów ADN" w zakresie koniecznym dla wypełnienia określonych ustawą z dnia 19 sierpnia 2011 r. o przewozie towarów niebezpiecznych (tekst pierwotny: Dz. U. z 2011 r. Nr 227 poz. 1367) zadań Dyrektora urzędu żeglugi śródlądowej – stosownie do postanowień art. 34 ust. 2 ww. ustawy jest znacząco mniejszy, niż zawarty w dowodzie tożsamości.

2) *wzór świadectwa eksperta ADN,* w zakresie pozycji „Narodowość". Pozycja ta powinna była zostać zastąpiona pozycją „Obywatelstwo".

Narodowość jest stanem świadomości każdego człowieka i wynikającą z tego stanu jego identyfikacją z daną grupą etniczną. Informacja o narodowości wprost ujawnia zatem pochodzenie etniczne, a niekiedy także rasowe człowieka, co przesądza o uznaniu przetwarzania danych o narodowości za przetwarzanie danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych. Dla przetwarzania tej danej osobowej („narodowości") konieczna jest przesłanka legalności przetwarzania danych osobowych w postaci aktu prawa rangi ustawy. Podkreślić też należy, iż dla dopełnienia obowiązków wynikających z przepisów ustawy o przewozie towarów niebezpiecznych jest to informacja całkowicie zbędna.

Powyższe uwagi zostały uwzględnione. Rozporządzenie zostało opublikowane w Dz. U. z 2015 r. poz. 629.

W projekcie **rozporządzenia Ministra Obrony Narodowej w sprawie ewidencji wojskowej żołnierzy pełniących służbę kandydacką**[298] zastrzeżenia organu ds. ochrony danych osobowych wzbudziły:

1) § 6 ust. 4 stanowiący o „jawności" teczki akt personalnych, karty ewidencyjnej i karty wypożyczeń teczki akt personalnych, w związku z § 1 pkt 3 projektu stanowiącym o przetwarzaniu „niejawnego" zbioru danych kandydatów na

[298] DOLiS-033-210/14.

żołnierzy. Wątpliwość powstała w związku z tym, iż wydaje się, że dane osobowe ujęte w tych dokumentach nie stanowią informacji „jawnych" (w rozumieniu publicznie dostępnych, czy powszechnie dostępnych), lecz co najwyżej takich, którym nie nadano klauzuli tajności, tym bardziej, że § 17 i kolejnych określa się komu, i na jakich zasadach zawierające dane osobowe dokumenty mogą być udostępniane. Wydaje się więc, iż usunięcie zdania pierwszego w § 6 ust. 4 nie spowodowałoby zmiany postanowień przepisu.

2) § 8, w szczególności w zakresie tego, czy teczka akt personalnych obejmuje kartę ewidencyjną, czy też należy wprowadzić regulacje podobne do zastosowanych w drugim, opiniowanym poniżej projekcie.
3) § 11 w zakresie celowości zamieszczenia jego pkt. 1. Jako, że informacje, o których mowa była w § 11 pkt 2-8 stanowią dane osobowe, uzasadnionym wydawało się nadanie § 11 zdanie wstępne brzmienia: „W ewidencji elektronicznej gromadzi się dane osobowe oraz informacje o zmianach tych danych w zakresie:" i rezygnację z zapisu obecnego punktu 1.
4) § 17 zdanie wstępne w zakresie wyrazów „zgodnie z przepisami ustawy o ochronie danych osobowych", bowiem takie zastrzeżenie było zupełnie zbędne.
5) § 19 pkt 2. Niejasnym było, czy pokwitowanie udostępnienia karty ewidencyjnej ma się znajdować w teczce akt personalnych.
6) załącznik nr 2, o którym mowa w § 3 pkt 2 projektu, w zakresie pozycji „narodowość". Pozycja ta powinna dotyczyć „obywatelstwa", nie zaś narodowości - zgodnie z art. 132a ust. 3 ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (t. j. Dz. U. z 2010 r. Nr 90, poz. 593 z późn. zm.).

Zgodnie z art. 132a ust. 3 ustawy o służbie wojskowej żołnierzy zawodowych dopuszczalne jest jedynie przetwarzanie danych o obywatelstwie, nie zaś narodowości żołnierzy zawodowych. Tych dwóch pojęć nie można przy tym utożsamiać, gdyż pojęcie obywatelstwa jest jednoznacznie określone przez prawo (w Rzeczypospolitej Polskiej – przez ustawę z dnia 15 lutego 1962 roku o obywatelstwie polskim – t. j. Dz. U. z 2012 r. poz. 161 z późn. zm.), a narodowość jest stanem świadomości każdego człowieka i wynikającą z tego stanu jego identyfikacją z daną grupą etniczną. Informacja o narodowości wprost ujawnia zatem pochodzenie etniczne, a niekiedy także rasowe człowieka, co przesądza o uznaniu przetwarzania danych o narodowości za przetwarzanie danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych. W tym stanie rzeczy,

przepisy art. 132a ustawy o służbie wojskowej żołnierzy zawodowych stanowią *lex specialis* wobec postanowień rozdziału 3 ustawy o ochronie danych osobowych i muszą być interpretowane w sposób ścisły, regulacje przewidziane w akcie prawnym o randze niższej niż ustawa nie mogą nakazywać zbierania w ewidencji wojskowej danych innych, aniżeli wprost wymienione w art. 132a ust. 2 i 3 ustawy o służbie wojskowej żołnierzy zawodowych. Powyższe rozporządzenie zostało opublikowane w Dz. U. z 2014 r. poz. 1637.

W projekcie **rozporządzenia Ministra Obrony Narodowej w sprawie ewidencji wojskowej żołnierzy zawodowych**[299] zastrzeżenia wzbudziły:

1) § 6 ust. 6 stanowiący o „jawności" teczki akt personalnych i karty wypożyczeń teczki akt personalnych, w związku z § 1 pkt 4 projektu stanowiącym o przetwarzaniu „niejawnego" zbioru danych żołnierzy (podobnie jak w projekcie dot. kandydatów na żołnierzy).
2) pozycja 5 załącznika nr 2, o którym mowa w § 3 pkt 2, oraz pozycja 2 załącznika nr 4, o którym mowa w § 8 ust. 5 pkt 1 projektu, w zakresie w jakim przetwarzane mają być informacje o narodowości żołnierza. W myśl – regulującego kwestie związane z przetwarzaniem w ewidencji wojskowej danych żołnierzy zawodowych – art. 48 ustawy o służbie wojskowej żołnierzy zawodowych dopuszczalne jest jedynie przetwarzanie danych o obywatelstwie, nie zaś narodowości żołnierzy zawodowych.
3) pozycja 4 załącznika nr 2, o którym mowa w § 3 pkt 2 projektu, dotyczącej numeru NIP. W obecnym stanie prawnym posługiwanie się tym numerem (o ile został nadany) jest zbędne.
4) § 17 w zakresie celowości zamieszczenia jego pkt. 1. Z uwagi na to, że informacje, - o których mowa w § 17 pkt 2-10 stanowią dane osobowe, uzasadnionym redakcyjnie wydawał się podział § 17 na ustępy 1 i 2. Nadanie § 17 ust. 1 brzmienia: „W ewidencji elektronicznej gromadzi się dane osobowe i informacje o zmianach tych danych w zakresie:". Nadanie § 17 ust. 2 brzmienia: „W ewidencji elektronicznej prowadzi się księgę etatową jednostki wojskowej, której wzór określa załącznik nr 7."
5) § 28 zdanie wstępne w zakresie wyrazów „zgodnie z przepisami ustawy o ochronie danych osobowych", bowiem takie zastrzeżenie jest zupełnie zbędne.

[299] DOLiS-033-210/14.

Podobnie jak w projekcie dot. kandydatów na żołnierzy podstawę prawną przetwarzania danych osobowych będą stanowić przepisy projektowanego rozporządzenia, stanowiące przesłankę przetwarzania danych, o której mowa w art. 23 ust. 1 pkt 2, i art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, i zarazem *lex specialis* wobec postanowień tej ustawy. Rozporządzenie to zostało opublikowane w Dz. U. z 2014 r. poz. 1638.

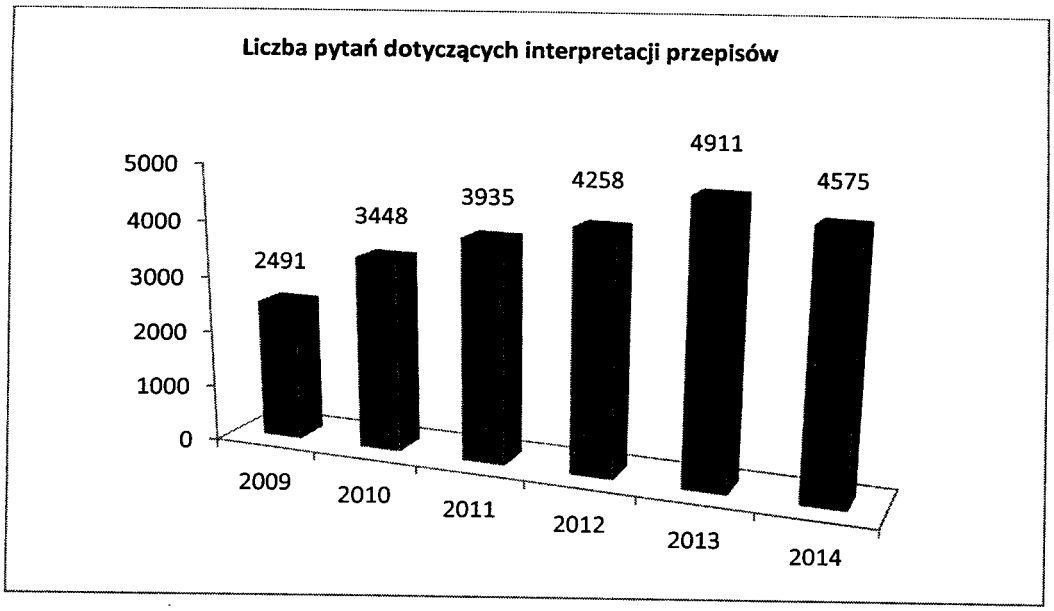
8. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

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 2014 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **4575 pytań prawnych** z prośbą o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, bądź sygnalizujących różnego rodzaju problemy interpretacyjne związane z ich przestrzeganiem.



Wykres 33: ***Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach - 2011–2014.***

Wartym zauważenia jest, iż liczba zapytań dotyczących interpretacji przepisów prawa w 2014 r. w porównaniu do roku 2013 zmniejszyła się o prawie 7%. Tym samym, dotychczasowa z roku na rok tendencja wzrostowa liczby wpływającej do Biura Generalnego Inspektora Ochrony Danych Osobowych (Biura GIODO) korespondencji stanowiącej zapytania nie była kontynuowana.

Stąd należy wnosić, że działania o charakterze informacyjnym i edukacyjnym realizowane przez organ do spraw ochrony danych osobowych przynoszą potrzebne rezultaty, co jednak nie oznacza, że zainteresowanie pozyskiwaniem informacji w formie odpowiedzi - na pytania znacząco spadło, czy – tym bardziej – nie jest oczekiwane.

8.1.1. Administracja publiczna

W 2014 r. wiele wątpliwości osób kierujących pytania do Generalnego Inspektora Ochrony Danych Osobowych budziły kwestie dotyczące upubliczniania, w tym na stronach internetowych, informacji o charakterze osobowym, oraz udostępniania danych osobowych. Nadal także wiele wątpliwości dotyczyło pozyskiwania, w związku z prowadzoną działalnością, danych osobowych bez podstawy prawnej, lub w zakresie szerszym, niż przewidziany przepisami prawa.

Jako przykład sprawy dotyczącej ujawnienia danych osobowych przy użyciu poczty elektronicznej można wskazać zapytanie **o legalność ujawniania numerów PESEL pracowników Urzędu Nadzoru Finansowego w procesie realizacji obowiązku udzielania odpowiedzi za pomocą środków komunikacji elektronicznej wg postanowień ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw**[300].

W odpowiedzi poinformowano, że przedstawiony problem jest Generalnemu Inspektorowi dobrze znany i był sygnalizowany przez ten organ przede wszystkim w ramach prac nad projektem *rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym*[301]. Stanowisko GIODO podnoszone w trakcie powyższych prac stanowiło jednocześnie wyjasnienie kwestii związanych z tym zagadnieniem.

W trakcie powyższych prac Generalny Inspektor Ochrony Danych Osobowych podnosił bowiem, że stosowanie aktualnych mechanizmów uwierzytelnienia za pomocą numeru PESEL przy jednoczesnym braku możliwości skorzystania z jakiegokolwiek alternatywnego rozwiązania w tym zakresie (posłużenia się innego rodzaju daną osobową) budzi w naszym kraju duże kontrowersje. O ile zrozumiała jest konieczność użycia tego numeru w przypadku weryfikacji osoby wnioskującej o wydanie certyfikatu oraz obecność tego rodzaju danej w zestawie danych przypisanych do wydanego certyfikatu, to zdecydowanie sporna jest konieczność ujawniania nr PESEL innym osobom. GIODO wskazywał, że problem ten nasilił się w Polsce w związku z wejściem w życie ustawy z dnia 29 lipca 2011 r. o zmianie ustawy - o zasadach ewidencji i identyfikacji podatników i płatników oraz niektórych innych ustaw - (Dz. U. nr 171, poz. 1016). Obecnie jedynym identyfikatorem osób fizycznych, która nie prowadzi działalności gospodarczej, jest numer PESEL.[302] Od dnia 1 stycznia 2012 r. także identyfikatorem podatkowym jest numer PESEL. W konsekwencji wszystkie osoby, które nie miały prawa posługiwania się numerem NIP, zmuszone były do ujawniania numeru PESEL przy posługiwaniu się podpisem elektronicznym.

---

[300] DOLiS-072-36/14.

[301] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U.UE L z dnia 28 sierpnia 2014 r. 2014.257.73).

[302] Art. 67 ustawy o zmianie ustawy o zasadach ewidencji i identyfikacji podatników i płatników oraz niektórych innych ustaw stanowi, że z dniem 1 stycznia 2012 r. znosi się numer identyfikacji podatkowej nadany osobom fizycznym objętym rejestrem PESEL, nieprowadzącym działalności gospodarczej lub niebędącym zarejestrowanymi podatnikami podatku od towarów i usług.

Ponadto, zgodnie z art. 15 ustęp 1 ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2011 r., Nr 197, poz. 1172 z późn. zm.) podstawę do opublikowania aktu stanowi on sam w formie dokumentu elektronicznego opatrzonego bezpiecznym podpisem elektronicznym[303]. W konsekwencji, w dziennikach urzędowych części ministerstw i województw znajdują się dane osobowe urzędników, z którymi zapoznać się może każdy internauta sprawdzający, kto podpisał dany dokument. Zdaniem GIODO wystarczającym dla jednoznacznej identyfikacji tych osób byłoby jedynie wskazanie instytucji, w której są one zatrudnione i pełnionej przez nie funkcji, czy zajmowanego stanowiska. Nie jest natomiast konieczne w tym celu wykorzystywanie cechy identyfikacyjnej związanej z prywatnością tej osoby.

Analogiczne uwagi organ ochrony danych osobowych zgłosił w odniesieniu do posługiwania się profilem zaufanym użytkownika na platformie ePUAP, co również wiąże się z koniecznością ujawniania numeru PESEL. Generalny Inspektor podkreślił, że udogodnienia oparte na identyfikacji osób w systemach e-government, zarówno w odniesieniu do urzędników, jak i innych osób, np. przy rejestracji działalności gospodarczej, nie mogą następować kosztem naruszenia konstytucyjnie chronionych praw i wolności. Zastosowanie numeru PESEL może naruszyć prywatność danych osobowych obywatela poprzez możliwość powiązania z innymi rejestrami oraz z uwagi na semantyczność cech tego identyfikatora (data urodzenia i płeć). Należy również pamiętać, że na podstawie prawa do ponownego wykorzystania informacji publicznej będzie można przetwarzać taką informację w dowolnym komercyjnym lub niekomercyjnym celu (rozdział 2a znowelizowanej ustawy o dostępie do informacji publicznej stanowiący implementację dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego DZ.U.UE L z dnia 31 grudnia 2003 r.). Ponadto za pomocą numeru PESEL znacznie ułatwione jest „profilowanie" użytkownika Internetu. Stąd w opinii Generalnego Inspektora konieczne było rzetelne rozważenie zagadnienia zakresu danych wykorzystywanych w powyższych sytuacjach, z uwzględnieniem zasady adekwatności danych, a zatem ograniczenia zakresu danych do niezbędnego dla realizacji ściśle

[303] Art. 15 ust. 1 ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych stanowi, iż podstawą do ogłoszenia aktu normatywnego lub innego aktu prawnego jest akt w formie dokumentu elektronicznego opatrzony przez upoważniony do wydania aktu organ bezpiecznym podpisem elektronicznym, - w rozumieniu przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.[2)]), weryfikowanym przy pomocy kwalifikowanego certyfikatu, zwanym dalej "bezpiecznym podpisem elektronicznym".

określonego celu[304]. Należy poszukiwać innych efektywnych rozwiązań w tym zakresie - np. wykorzystywanie w tym celu innego rodzaju numeru pozwalającego na uwierzytelnianie ważności certyfikatu i tożsamości osoby podpisującej się podpisem elektronicznym, przy zastosowaniu rozwiązania, że szerszy zestaw danych osobowych, w tym numer PESEL, byłby dostępny do wiadomości podmiotu świadczącego usługi certyfikacyjne.

Warto w tym miejscu wspomnieć, iż w czerwcu 2014 r. Generalny Inspektor opiniując przekazane mu przez Ministerstwo Gospodarki projekty rozporządzeń wykonawczych do ustawy z dnia 18 września 2001 r. o podpisie elektronicznym m.in. projekt *rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*, odnotował z satysfakcją niektóre z proponowanych w tym projekcie rozwiązań. W projekcie rozporządzenia rozszerzono bowiem listę używanych obecnie identyfikatorów (NIP lub PESEL) o dodatkowe identyfikatory, takie jak numer dowodu tożsamości i numer paszportu, co powinno skutkować tym, że nie będzie obowiązku podawania przez subskrybenta nr PESEL w celu uzyskania certyfikatu kwalifikowanego.[305]

Wiele zapytań dotyczyło **udostępniania informacji publicznej[306]**. W tej materii Generalny Inspektor informacje przedstawiał jedynie pomocniczo. Mając bowiem na względzie zakres kompetencji GIODO określony w przepisach ustawy o ochronie danych osobowych nie jest on organem uprawnionym do zajmowania stanowiska i rozstrzygania w sprawach podlegających rozpatrzeniu w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.), w odniesieniu do informacji publicznej, której nie jest dysponentem. Generalny Inspektor, stosownie do przyznanych mu kompetencji, nie może podejmować czynności dotyczących postępowań prowadzonych przez inne podmioty na podstawie właściwych przepisów prawa. Dotyczy to zarówno merytorycznej odmowy, czy udostępnienia informacji publicznej, jej formy, czy też

---

[304] Zgodnie z art. 26 ustęp 1 pkt 3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

[305] Jak wynika z informacji publikowanych na stronach Rządowego Centrum Legislacji prace nad przedmiotowym rozporządzeniem są w toku (stan na czerwiec 2015 r.).

[306] Np. DOLiS. 035-131/14, DOLiS-035-4088/14

ewentualnych dalszych działań związanych z okolicznością uzyskania rozstrzygnięcia w tym względzie przez sądem powszechnym[307].

Generalny Inspektor informował, że prawo dostępu do informacji publicznej ma charakter zasady, a podlega ograniczeniu w zakresie i na zasadach określonych w przepisach powołanej ustawy (ochrona informacji niejawnych, innych tajemnic ustawowo chronionych, prywatności osoby fizycznej lub tajemnicy przedsiębiorcy). Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa[308].

Ustawa o dostępie do informacji publicznej konkretyzuje, wyrażone w art. 61 Konstytucji Rzeczypospolitej Polskiej, 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. Przepisy powyższe wymuszają konieczność każdorazowej oceny w przypadku udostępnienia informacji publicznej, czy określone informacje mieszczą się w zakresie pojęcia informacji publicznej i czy ich udostępnienie jest prawnie dopuszczalne. W każdym przypadku o udostępnieniu informacji publicznej rozstrzyga podmiot, w którego dyspozycji informacje te się znajdują. W jego gestii, a nie Generalnego Inspektora Ochrony Danych Osobowych pozostaje ocena, czy określone informacje mieszczą się w zakresie pojęcia informacji publicznej i czy ich udostępnienie na gruncie przepisów wyżej powołanej ustawy jest prawnie dopuszczalne. Następnie rozstrzygnięcie to podlega weryfikacji przez **sąd administracyjny**. Poddanie rozstrzygnięć podmiotów zobowiązanych do udostępnienia informacji publicznej zaskarżeniu do sądu administracyjnego jest uzasadnione z jednej strony wagą zasady jawności działania organów państwa, która jest uważana za jedną z fundamentalnych i konstytucyjnych wartości państwa prawa, z drugiej właśnie stopniem skomplikowania tej materii i trudnością w podejmowaniu rozstrzygnięć w tym zakresie.[309]

---

[307] Co znajduje potwierdzenie w orzecznictwie Naczelnego Sądu Administracyjnego, np. w wyroku NSA z dnia 2 marca 2001 r. (sygn. akt II SA 401/00), w którym NSA stwierdził, że: „Generalny Inspektor Ochrony Danych Osobowych, (...), nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji czy w inny sposób określony odpowiednimi procedurami."

[308] Zgodnie z art. 5 ust. 1 i 2 ustawy o dostępie do informacji publicznej.

[309] Powyższe znajduje potwierdzenie w cytowanym już wyroku NSA z dnia 2 marca 2001 r. (sygn. akt II SA 401/00), w którym NSA stwierdził, że: „Generalny Inspektor Ochrony Danych Osobowych, (...), nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w

Kwestię tę warto podnieść w niniejszym sprawozdaniu, gdyż w omawianym okresie sprawozdawczym do Biura GIODO wpłynęło ok. 100 zapytań dotyczących udostępnienia informacji publicznej zawierającej dane osobowe, w tym od centralnych organów publicznych,[310] które wydają się nie zdawać w pełni sprawy z zakresu uprawnień Generalnego Inspektora Ochrony danych Osobowych w tej materii.

Odnośnie prośby o zajęcie stanowiska **w przedmiocie prawnej możliwości przetwarzania przez Policję danych osobowych pokrzywdzonych przestępstwem oraz zawiadamiających o przestępstwie, w ramach rejestrów prowadzonych w Policji na potrzeby postępowań przygotowawczych** w sprawach karnych[311] poinformowano podmiot zainteresowany (Policję), że w ocenie Generalnego Inspektora Ochrony Danych Osobowych najważniejszym zagadnieniem związanym z inicjatywą mającą na celu wypracowanie założeń do budowy narzędzia informatycznego „wspierającego dokumentowanie czynności dochodzeniowo-śledczych oraz czynności rejestracyjne", służącego do przetwarzania danych osobowych pokrzywdzonych przestępstwem i zawiadamiających o przestępstwie jest kwestia podstawy prawnej dla przetwarzania danych osobowych, które mogą mieć status szczególnie chronionych[312].

Udzielając w tej sprawie odpowiedzi Generalny Inspektor wskazał, iż w chwili obecnej istnieją wątpliwości dotyczące braku w obowiązujących przepisach prawa odpowiedniej i wystarczającej podstawy prawnej uprawniającej Policję do tworzenia zbioru (przetwarzania w osobnym rejestrze) danych osób pokrzywdzonych przestępstwem i zawiadamiających o przestępstwie. Stworzenie takiego rejestru wymaga zatem – w opinii Generalnego Inspektora Ochrony Danych Osobowych - rzetelnego rozważenia i uprzedniego wprowadzenia uregulowań w obowiązujących przepisach prawa, zarówno w zakresie samych podstaw prawnych takiego rejestru, jak i celu, zasad i sposobu jego prowadzenia. Tworzenie systemów centralnych musi bowiem bezwzględnie znajdować solidne podstawy w wystarczająco precyzyjnych przepisach prawa.

---

sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji czy w inny sposób określony odpowiednimi procedurami."

[310] Np. sprawa o sygn.: DOLiS-035-2363/14

[311] DOLiS-035-1213/14, dot. cyt. „Zawarte w rejestrze informacje o sposobie zakończenia postępowania, czynią z niego urządzenie ewidencjonujące przestępstwa, w stosunku do których Policja – pomimo formalnego zakończenia postępowania przygotowawczego – w dalszym ciągu ma obowiązek realizować czynności wykrywcze. (...) Prowadzony wykaz pozwala również na wstępną weryfikację, czy uzyskana informacja, ujawnione zdarzenie, czy też przestępstwo objęte zawiadomieniem nie było już przedmiotem postępowania karnego, co stanowi negatywną przesłankę procesową, wskazaną w art. 17 § 1 pkt 7 kpk – powaga rzeczy osądzonej".

[312] Por. przypis 32.

W omawianym okresie sprawozdawczym, **w związku z pismem Trybunału Konstytucyjnego[313] Przewodniczącej składu orzekającego o opinię GIODO w sprawie wniosku Rzecznika Praw Obywatelskich z dnia 19 lipca 2013 roku o stwierdzenie niezgodności art. 20 ust. 1 w związku z art. 19 ust. 1 ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 z późn. zm.) z art. 47 oraz art. 51 ust. 1, 2 i 5 w zw. z art. 31 ust. 3 oraz z art. 92 ust. 1 Konstytucji Rzeczypospolitej Polskiej**, w odpowiedzi[314] Generalny Inspektor podzielił zarzuty podniesione przez Rzecznika Praw Obywatelskich w skierowanym do Trybunału Konstytucyjnego wniosku.[315] Sprawa ta zakończyła się zaś wyrokiem z dnia 18 grudnia 2014 r. podzielającym zastrzeżenia RPO, tym samym także Generalnego Inspektora Ochrony Danych Osobowych.

Przetwarzanie danych osobowych w centralnych systemach informatycznych w kontekście konieczności przejrzystego i starannego unormowania zasad i sposobu tego procesu jest obecnie przedmiotem istotnej debaty społecznej w której aktywny udział bierze organ do spraw ochrony danych osobowych, w tym postępowań przed Trybunałem Konstytucyjnym w przypadkach, gdy systemy takie nie mają wystarczających podstaw prawnych.

Podkreślenia zaś wymaga, iż przyjęte ostatecznie w obowiązującej ustawie o systemie informacji w ochronie zdrowia rozwiązanie prawne, zgodnie z którym tworzenie przez ministra właściwego do spraw zdrowia rejestrów medycznych (zawierających – co oczywiste – dane o stanie zdrowia, czyli dane podlegające szczególnej ochronie) miałoby się odbywać - na podstawie aktów wykonawczych (rozporządzeń tegoż ministra) budziło zasadnicze wątpliwości organu do spraw ochrony danych osobowych w trakcie całego procesu legislacyjnego ustawy o systemie informacji w ochronie zdrowia. Wątpliwościom tym Generalny Inspektor Ochrony Danych Osobowych dawał wyraz zarówno w korespondencji

[313] Pismo z dnia 12 lutego 2014 r. o sygn. akt K 33/13

[314] Pismo GIODO z dnia 19 marca 2014 r. o sygn.: DOLiS-072-7/14/TG/21309.

[315] Sprawa w Trybunale Konstytucyjnym o sygn. akt K 33/13, dot. ustawy o systemie informacji w ochronie zdrowia, która w obecnym kształcie nie wyznacza przedmiotu poszczególnych rejestrów i nie wskazuje, jakich lub jakiego rodzaju zachorowań, chorób, stanu zdrowia, metod leczenia, diagnozowania, monitorowania postępów w leczeniu oraz zagrożeń związanych z występowaniem których chorób, mają one dotyczyć. Ponadto ustawa nie określa, jakie dane, mogą być przetwarzane w rejestrach tworzonych przez ministra. Zagadnienia te pozostawione zostały do rozstrzygnięcia ministrowi właściwemu do spraw zdrowia na poziomie rozporządzeń tworzących poszczególne rejestry. Zgodność powyższych rozwiązań z Konstytucją zakwestionował Rzecznik Praw Obywatelskich a zastrzeżenia te podzielił w toku postępowania przed Trybunałem Prokurator Generalny - oraz Generalny Inspektor Ochrony Danych Osobowych.

dotyczącej tej sprawy,[316] jak również w ustnych wystąpieniach Generalnego Inspektora Ochrony Danych Osobowych i jego przedstawicieli wygłaszanych na różnych forach. Niestety, argumentacja podniesiona przez Generalnego Inspektora Ochrony Danych Osobowych nie zyskała akceptacji ustawodawcy, który w trakcie prac dotyczących – wtedy jeszcze projektu – ustawy o systemie informacji w ochronie zdrowia prowadzonych w Parlamencie poprzestał na wprowadzeniu rozwiązań szczegółowych mających na celu zwiększenie poziomu ochrony praw osób, których dane będą przetwarzane w rejestrach medycznych,[317] nie odstąpił wszakże od samej koncepcji tworzenia rejestrów medycznych na podstawie rozporządzeń ministra właściwego do spraw zdrowia.

Generalny Inspektor Ochrony Danych Osobowych sygnalizował przedmiotowy problem również Rzecznikowi Praw Obywatelskich[318] co być może stanowiło dodatkowy asumpt do złożenia do Trybunału Konstytucyjnego przez Rzecznika Praw Obywatelskich wniosku z dnia 19 lipca 2013 roku.

W 2014 r. Ministerstwo Zdrowia zainicjowało – wysoce istotną z punktu widzenia problematyki ochrony danych osobowych – zmianę przepisów odnoszących się do systemu informacji w ochronie zdrowia, mianowicie projekt **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**. Uwagi Generalnego Inspektora zostały uwzględnione w tym projekcie[319].

Generalny Inspektor ustosunkowywał się również do **zapytania dotyczącego uprawnień do przetwarzania danych osobowych przez organy jednostek samorządu terytorialnego udzielające dotacji, w trakcie kontroli prawidłowości ich wykorzystywania, a przyznawanych niepublicznym szkołom i placówkom oświatowym**[320].

W odpowiedzi wyjaśniono, że odrębne w stosunku do ustawy o ochronie danych osobowych przepisy regulujące realizację określonych zadań organów jednostek samorządu terytorialnego, w tym przypadku – zadań w zakresie oświaty, oraz ewentualnie akty prawa

---

[316] Pisma skierowane do Ministerstwa Zdrowia (pismo z dnia 9 września 2010 roku o sygn. DOLiS-033-338/10/36114 – teza 14; pismo z dnia 12 października 2010 roku o sygn. DOLiS-033-338/10/40146 – tezy 3 i 4), jak i pisma skierowane do Sejmu Rzeczypospolitej Polskiej (pismo z dnia 15 października 2010 roku o sygn. DOLiS-033-338/10/42177 – teza I i II; pismo z dnia 15 marca 2011 roku o sygn. DOLiS-033-338/10/11535/11 – tezy 5, 11 i 12).

[317] Np. art. 19 ust. 9 ustawy o systemie informacji w ochronie zdrowia dotyczący sui generis obowiązku informacyjnego.

[318] Pismo z dnia 18 lutego 2011 roku o sygn. DOLiS-033-338/10/6346/11.

[319] W wersji z dnia 17.02.2015 r. Szerzej na ten temat w części sprawozdania dotyczącej prac legislacyjnych, odnośnie sprawy o sygn.: DOLiS-033-340/15.

[320] DOLiS-035-3108/14.

miejscowego dotyczące dotacji dla przedszkoli. Przepisy ustawy z dnia 7 września 1991 r. o systemie oświaty (t.j. Dz. U. z 2004 r. Nr 256 poz. 2572 z późn. zm.) zobowiązują organ stanowiący jednostki samorządu terytorialnego do ustalenia trybu udzielania i rozliczania dotacji oraz trybu i zakresu kontroli prawidłowości ich wykorzystywania, uwzględniając w szczególności podstawy obliczania dotacji, zakres danych, które powinny być zawarte we wniosku o udzielenie dotacji i w rozliczeniu jej wykorzystania, oraz termin i sposób rozliczenia dotacji (art. 90 ust. 4 powołanej ustawy). Artykuł zaś 90 ust. 3f powołanej ustawy przewiduje prawo osób upoważnionych do przeprowadzania kontroli do wglądu do prowadzonej przez nie dokumentacji organizacyjnej i finansowej.

W odniesieniu do celów kontrolnych najczęściej powoływana jest generalna reguła, że zakres pozyskiwanych dla celów kontroli danych osobowych musi być adekwatny do przedmiotu kontroli i służyć jej celom. Udostępnienie danych osobowych w celach wynikających z odrębnych przepisów oraz w sposób w nich określony nie powinno być traktowane jako naruszenie ustawy o ochronie danych osobowych.

Kolejnym zagadnieniem, z którym w omawianym okresie sprawozdawczym spotkał się Generalny Inspektor, była **kwestia określenia podmiotu, na rzecz którego powinna być przekazana dokumentacja pracownicza pozostawiona na terenie nieruchomości przejętej przez gminę**[321].

W tej sprawie wskazano pytającemu, iż właściwym wydaje się poinformowanie o zaistniałej sytuacji Naczelnego Dyrektora Archiwów Państwowych, który - działając w pierwszej kolejności na podstawie ustawy o narodowym zasobie archiwalnym i archiwach – może wydać decyzję nakazującą złożenie dokumentacji, która należała do pracodawcy wykreślonego z Krajowego Rejestru Sądowego lub z ewidencji działalności gospodarczej, na odpłatne przechowywanie we wskazanym archiwum państwowym, jeżeli istnieje zagrożenie jej zniszczenia, w szczególności na skutek oddziaływania czynników atmosferycznych lub bezprawnego działania osób trzecich, a brak jest podstaw prawnych do jej przekazania innemu podmiotowi do dalszego przechowywania. Przed wydaniem decyzji Naczelny Dyrektor Archiwów Państwowych dokonuje oceny dokumentacji w miejscu, w którym się ona znajduje. Decyzji tej nadaje się rygor natychmiastowej wykonalności[322].

---

[321] DOLiS-035-6/14.

[322] Stanowi o tym art. 51z ustawy o ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tekst jednolity: Dz. U. z 2011 r. Nr 123 poz. 698 z późn. zm.)

Jednocześnie wyjaśniono, że przepisy ustawy o ochronie danych osobowych nie regulują zasad posługiwania się dokumentami, w tym dokumentacją pracowniczą prowadzoną przez przedsiębiorcę. Ustawa o ochronie danych osobowych reguluje zasady przetwarzania, w tym ochrony danych osobowych.[323]

Generalny Inspektor pozytywnie natomiast ocenił dokonanie zawiadomienia właściwych organów ścigania o możliwości popełnienia przestępstwa, o podjęciu bowiem takiego działania poinformowano GIODO. Przepisy karne ustawy o ochronie danych osobowych stanowią o penalizacji choćby nieumyślnego naruszenia obowiązku zabezpieczenia danych osobowych przed ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,[324] o czym administratorzy danych osobowych powinni zdawać sobie sprawę.[325]

W 2014 r. do Generalnego Inspektora zwrócił się **powiatowy urząd pracy z prośbą o stanowisko w sprawie udostępnienia danych osobowych bezrobotnych dla firmy zewnętrznej prowadzącej badanie socjologiczne**[326].

Badanie – prowadzone przez wojewódzki urząd pracy zgodnie z umową, jaką zawarł z firmą zewnętrzną – miało dotyczyć diagnozy efektywności staży zawodowych na terenie województwa. Udostępnienie danych miało się odbyć na podstawie umowy powierzenia przetwarzania danych osobowych - tj. rozwiązania przewidzianego przepisami ustawy o ochronie danych osobowych - zawartej między powiatowym urzędem pracy a podmiotem prowadzącym badania.

W odpowiedzi GIODO wskazał, że w przypadku udostępnienia danych osobowych, koniecznym jest posiadanie przesłanki legalności ich przetwarzania, jednak takiej podstawy nie może stanowić określający zasady powierzenia danych osobowych art. 31 ustawy o

[323] Powyższe znajduje potwierdzenie w utrwalonym orzecznictwie sądów administracyjnych, np. w wyroku z dnia 6 września 2005 r. (sygn. II SA/Wa 825/05) Wojewódzki Sąd Administracyjny w Warszawie orzekł, że „W ustawie o ochronie danych osobowych brak jest przepisów obligujących administratora do udostępnienia dokumentów zawierających dane osobowe. Ustawodawca posługuje się pojęciem „udostępnienia", odnosząc je zawsze do danych osobowych, a nie zawierających je dokumentów." Jednocześnie w ocenie sądu „(...) kwestia udostępniania dokumentów znajdujących się w aktach osobowych pracownika, nie jest w ogóle objęta regulacją ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i nie może być na jej gruncie rozpatrywana".

[324] Zgodnie bowiem z art. 51 ustawy o ochronie danych osobowych, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (ust. 1); jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności - do roku. Z kolei art. 52 ustawy stanowi, iż 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.

[325] Jednakże prowadzenie spraw karnych nie należy do kompetencji GIODO. Por. wyrok NSA z dnia 2 marca 2001 r. (sygn. akt II SA 401/00).

[326] DOLiS-035-1854/14

ochronie danych osobowych. Istotą instytucji powierzenia przetwarzania danych, o której mowa w tym przepisie, jest podjęcie przetwarzania danych osobowych w imieniu i na rzecz administratora danych[327]. Umowa taka musi określać zakres i cel przetwarzania danych, które zostały powierzone, takim zaś celem nie może być dokonywanie operacji na danych osobowych, według potrzeb, czy nawet regulowanych przepisami prawa zadań podmiotu innego, niż administrator danych, który te dane powierza. Taka natomiast (niedozwolona) sytuacja mogła miejsce, gdy powiatowy urząd pracy (administrator danych) powierzy podmiotowi zewnętrznemu (wykonawcy badania) dane osobowe w celu przeprowadzenia badania na rzecz innego podmiotu, w tym wypadku wojewódzkiego urzędu pracy. Powierzenie przetwarzania danych osobowych oznacza dokonywanie na danych operacji jedynie w imieniu i na rzecz ich administratora i nie może prowadzić do zmiany jego statusu, tj. podejmowania przez podmiot, któremu powierzono przetwarzanie danych, jakichkolwiek operacji na tych danych, które to działania prowadziłyby do realizacji celów lub interesów innego podmiotu.

Umowa powierzenia może dotyczyć tylko i wyłącznie sposobu przetwarzania danych osobowych, a nie realizacji kompetencji innego podmiotu i zarazem nie może stanowić o przekazaniu kompetencji administratora danych osobowych. Jednocześnie art. 31 ustawy o ochronie danych osobowych nie może zastępować podstawy prawnej legalizującej proces przetwarzania danych osobowych. Administrator może powierzyć przetwarzanie tylko tych danych, których jest dysponentem, a w przypadku związania przepisami szczególnymi – tylko o ile wynika to z przepisów prawa. Z uwagi na powyższe, organ nie powinien wykorzystywać posiadanych danych osobowych dla celów innych niż realizacji wyznaczonych temu organowi przepisami prawa zadań czy kompetencji[328].

Nie znajduje więc uzasadnienia przekazywanie danych przez powiatowy urząd pracy innemu podmiotowi w celu realizacji zadań zleconych temu podmiotowi przez wojewódzki urząd pracy. Taka konstrukcja nie znajduje podstaw w przepisach obowiązującego prawa, a zwłaszcza nie można wywodzić jej dopuszczalności z treści art. 31 ustawy o ochronie danych osobowych.

---

[327] Zgodnie z art. 31 ustawy o ochronie danych osobowych administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Podmiot ten może przetwarzać dane wyłącznie w celu i zakresie przewidzianym w umowie (art. 31 ust. 2)

[328] Dla tej sytuacji należy mieć również na uwadze zasadę legalizmu, wyrażoną zarówno w przepisach Konstytucji RP (art. 7), jak i ustawy Kodeks postępowania administracyjnego (art. 6.

Konkludując, zarówno powiatowy urząd pracy jak i wojewódzki urząd pracy mogą powierzać przetwarzanie, ale wyłącznie własnych danych i dla realizacji własnych celów podmiotowi zewnętrznemu, przy wyraźnym określeniu tych celów w przepisach prawa rangi ustawy.

8.1.2. Szkolnictwo.

W zakresie spraw dotyczących szkolnictwa w omawianym okresie sprawozdawczym do GIODO kierowano również prośby o interpretację przepisów ustawy Prawo o szkolnictwie wyższym, w zakresie przetwarzania adresu do korespondencji w celu prowadzenia monitoringu karier zawodowych, a mianowicie **czy uczelnia może wysyłać ankiety bez zgody na pozyskany od studenta w czasie studiów adres e-mail** (czy ten adres można traktować jako „adres do korespondencji" w rozumieniu przepisów ustawy)[329]. Pytanie zostało skierowane przez biuro karier jednej z uczelni wyższych[330].

Przepisy prawa regulujące zasady monitorowania losów absolwentów zawarte są w ustawie z dnia z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2012 r. poz. 572 z późn. zm.). W celu dostosowania programu kształcenia do potrzeb rynku pracy uczelnia może zaś prowadzić własny monitoring karier zawodowych swoich absolwentów. W celu prowadzenia monitoringu, uczelnia może przetwarzać dane osobowe absolwentów obejmujące imiona i nazwisko oraz adres do korespondencji.[331]. Biorąc pod uwagę uregulowania ww. aktu prawnego dotyczące zakresu przetwarzanych danych osobowych absolwentów, wydaje się jednak, iż adres do korespondencji powinien być na gruncie przedmiotowej ustawy traktowany jako (tradycyjny) adres pocztowy. Katalog bowiem danych przekazywanych w właśnie w związku z monitorowaniem losów absolwentów np. przekazywanych ministrowi właściwemu do spraw szkolnictwa wyższego przez Zakład Ubezpieczeń Społecznych, obejmuje pierwsze trzy cyfry kodu pocztowego adresu zameldowania lub adresu zamieszkania, lub adresu do korespondencji osoby ubezpieczonej[332].

Wynikające z przepisów szczególnych upoważnienie uczelni do przetwarzania danych absolwentów obejmuje zatem ograniczony zakres ich danych. W pozostałym zakresie,

---

[329] DOLiS-035-3346/14

[330] Zgodnie z art. 13b ust. 12 ustawy z dnia z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. z 2012 r., poz. 572, z późn. zm.), celu dostosowania programu kształcenia do potrzeb rynku pracy uczelnia może prowadzić własny monitoring karier zawodowych swoich absolwentów.

[331] Zgodnie z artykułem 13b ust. 13 ustawy prawo o szkolnictwie wyższym.

[332] Zgodnie z artykułem 13b ust. 3 pkt 4 ustawy prawo o szkolnictwie wyższym.

również w przypadku przetwarzania adresów poczty elektronicznej, konieczne jest więc odniesienie się do przepisów ustawy o ochronie danych osobowych, tzn. posiadanie przez uczelnię przesłanki określonej w art. 23 ust. 1 ustawy dla przetwarzania także takiej danej osobowej.

Innym ciekawym zagadnieniem istotnym w dziedzinie szkolnictwa oraz dla budowy mechanizmów służących komunikacji elektronicznej była **kwestia dopuszczalności udostępnienia firmie, której powierzono w związku z budową i obsługą systemu przetwarzanie danych osobowych, w tym numeru PESEL potencjalnych użytkowników systemu, celem ich rozpoznania przez system** przy pierwszym logowaniu. Sprawa ta także dotyczyła szkolnictwa, bowiem wdrożenia dzienników elektronicznych w szkole i kwestii pierwszego logowania rodziców dzieci, ma ona jednak wymiar uniwersalny[333].
W tej sprawie wyjaśniono, iż wykorzystywanie nr PESEL, nawet podczas pierwszego logowania się do systemu nie powinno mieć miejsca. Istnieją bowiem inne (proste) metody generowania i następnie doręczania użytkownikom systemu właściwie zindywidualizowanych (pierwszych) loginów i haseł, bez użycia ww. danej osobowej, która nie należy co prawda do tzw. danych szczególnie chronionych, lecz jest używana np. jako jednoznacznie identyfikująca strony umów w obrocie gospodarczym.

8.1.3. Instytucje finansowe.

W 2014 r. do GIODO zwróciła się Komisja Nadzoru Finansowego o **wyrażenie stanowiska w zakresie możliwości rozszerzenia treści wpisów dotyczących osób fizycznych o informacje dodatkowe związane z prowadzoną przez tę osobę działalnością**, np. nazwę portalu, za pośrednictwem którego osoba fizyczna prowadzi działalność, obszar terytorialny prowadzenia działalności lub podmiot, na rzecz którego jest prowadzona działalność, w sytuacji, gdy na podstawie art. 6b ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2012 r. poz. 1149), KNF jest zobowiązana do podania do publicznej wiadomości informacji o składanych zawiadomieniach o podejrzeniu popełnienia przestępstwa[334]. KNF zaznaczyła jednocześnie, iż powyższe rozszerzenie jest wskazane, bowiem nie następuje ujawnienie nazwiska osoby podejrzanej, ze względu na postanowienie art. 6b ust. 2 zdanie pierwsze ustawy o nadzorze nad rynkiem finansowym.

---

[333] DOLiS-035-1614/14

[334] Sygn. GIODO: DOLiS-035-1867/14, pismo KNF z dnia 29 kwietnia 2014 r. o sygn.: DKS/WK//063/29/1/MB.

W odpowiedzi wyjaśniono, iż zgodnie art. 6b ust. 2 ustawy o nadzorze nad rynkiem finansowym, Komisja podaje do publicznej wiadomości informację o złożeniu zawiadomienia o podejrzeniu popełnienia przestępstw określonych w ust. 1 tego artykułu, zaś informacja, o której mowa w ust. 1, zawiera firmę (nazwę) podmiotu, w związku z działalnością którego złożone zostało zawiadomienie o podejrzeniu popełnienia przestępstwa, a w przypadku gdy podmiot ten prowadzi działalność pod innym oznaczeniem, do publicznej wiadomości podaje się także to oznaczenie. Jednocześnie - jakkolwiek informacja, o której mowa w ust. 1, nie może zawierać danych osobowych[335] – należy też zauważyć, iż zgodnie z art. 43^2 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2014 r. poz. 121 z późn. zm.), przedsiębiorca działa pod firmą. Firmą zaś osoby fizycznej – zgodnie z art. 43^4 ustawy Kodeks cywilny - jest jej imię i nazwisko, co nie wyklucza włączenia do firmy pseudonimu lub określeń wskazujących na przedmiot działalności przedsiębiorcy, miejsce jej prowadzenia oraz innych określeń dowolnie obranych. Tym samym możliwe jest ujawnienie nazwiska przedsiębiorcy, o ile jest ono nazwą firmy, bądź częścią składową nazwy firmy.

Powyższe przepisy, stanowią *lex specialis* wobec przepisów ustawy o ochronie danych osobowych, i powinny być stosowane w pierwszej kolejności.

Kolejnym zagadnieniem podnoszonym przez Komisję Nadzoru Finansowego w jej korespondencji z organem do spraw ochrony danych osobowych, była **kwestia udostępnienia historii rachunku bankowego zmarłego klienta jego spadkobiercom[336].**

W tej sprawie Generalny Inspektor zauważył, iż zgodnie z przepisami ustawy Prawo bankowe, banku nie obowiązuje, z zastrzeżeniem ust. 4, zachowanie tajemnicy bankowej jedynie wobec osoby, której dotyczą informacje objęte tajemnicą.[337] Osobom trzecim informacje te mogą być ujawnione, wyłącznie gdy osoba, której informacje te dotyczą, na piśmie upoważni bank do przekazania określonych informacji wskazanej przez siebie osobie lub jednostce organizacyjnej[338].

Organ do spraw ochrony danych osobowych dostrzegł, iż bez uprzedniego poznania historii rachunku bankowego, spadkobiercy osoby zmarłej częstokroć nie mogą określić praw,

---

[335] Zgodnie z art. 6b ust. 2 zdanie pierwsze ustawy o nadzorze nad rynkiem finansowym.

[336] DOLiS-035-1743/14, pismo KNF z dnia 25 kwietnia 2014 r. o sygn.: DOK/WSII/0735/3/1/2014/AC

[337] Art. 104 ust. 3 ustawy Prawo bankowe z zastrzeżeniem ust. 4 tego artykułu. Należy też zauważyć, iż art. 922 § 1 i 2 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2014 r. poz. 121 z poźn. zm.), stanowią, iż prawa i obowiązki majątkowe zmarłego przechodzą z chwilą jego śmierci na jedną lub kilka osób stosownie do przepisów księgi niniejszej (§ 1). Nie należą do spadku prawa i obowiązki zmarłego ściśle związane z jego osobą, jak również prawa, które z chwilą jego śmierci przechodzą na oznaczone osoby niezależnie od tego, czy są one spadkobiercami (§ 2).

[338] Z zastrzeżeniem art. 105, 106a i 106b.

jakie im przysługują z tytułu dziedziczenia. Dostrzega też, iż w wielu przypadkach ujawnienie tych informacji może doprowadzić nie tylko do naruszenia przepisów dotyczących tajemnicy bankowej, ale też praw osób, których te dane dotyczą. Jednakże zajęcie w tych aspektach przedmiotowego zagadnienia jednoznacznego stanowiska wykracza poza przewidziane ustawą o ochronie danych osobowych kompetencje Generalnego Inspektora. Mogą się one stać natomiast przedmiotem rozważań Rzecznika Praw Obywatelskich, czy Urzędu Ochrony Konkurencji i Konsumentów.

Przypomniano także, iż ustawa o ochronie danych osobowych, określa zasady postępowania przy przetwarzaniu danych osobowych osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych[339]. Stosuje się ją tylko do danych osobowych osób fizycznych. Zgodnie bowiem z powszechnie obowiązującą wykładnią osobą fizyczną jest człowiek uczestniczący w stosunkach prawnych. Zdolność prawna człowieka, a tym samym zdolność do bycia podmiotem praw i obowiązków ustaje z chwilą jego śmierci. Wobec powyższego, ustawa o ochronie danych osobowych ma zastosowanie tylko do przetwarzanych danych osobowych osób żyjących.

Z kolei w aspekcie **okresu przechowywania informacji, w tym danych osobowych, gromadzonych w rejestrze transakcji[340], który instytucja obowiązana (np. bank) mocą przepisów ustawy *z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2014 r. poz. 455 z późn. zm.)* przeprowadzająca transakcję, ma obowiązek prowadzić**[341], Generalny Inspektor wyjaśnił, iż rejestr transakcji powinien być przechowywany przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, w którym transakcje zostały zarejestrowane[342]. Jednocześnie, informacje o transakcjach przeprowadzanych przez instytucje obowiązane oraz dokumenty dotyczące transakcji są przechowywane przez okres 5 lat, licząc od pierwszego dnia roku następującego po roku, w którym dokonano ostatniego zapisu związanego z transakcją. **Tym samym przepisy szczególne, regulujące kwestię prowadzenia rejestru** transakcji **nie**

[339] Zgodnie z art. 2 ust. 1 ustawy o ochronie danych osobowych.

[340] DOLiS-035-1123/14, pismo KNF z dnia 23 maja 2014 r.

[341] Co zgodnie z art. 8 ust. 1 i 3 dotyczy transakcji której równowartość przekracza 15.000 euro, a także 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, oraz takich, której okoliczności wskazują, że może ona mieć związek z praniem pieniędzy lub finansowaniem terroryzmu bez względu na jej wartość i charakter.

[342] W przypadku likwidacji, połączenia, podziału oraz przekształcenia instytucji obowiązanej, do przechowywania rejestrów i dokumentacji stosuje się odpowiednio przepisy art. *76* ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2013 .r, poz. 330 z późn. zm.).

przewidują możliwości dalszego przetwarzania danych osobowych zawartych w przedmiotowym rejestrze.

Stosownie do treści art. 26 ust. 1 pkt 1 i 4 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, oraz przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, **nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.** Celem zaś przetwarzania w przedmiotowej sprawie jest realizacja przepisów prawa, dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, z których nie wynika możliwość wydłużenia 5-letniego okresu przechowywania danych. Podkreślić należy, iż po upływie terminów wskazanych w ustawie, brak jest podstaw prawnych do dalszego przetwarzania danych osobowych zawartych w rejestrach, więc powinny zostać one w sposób trwały usunięte.[343] Okres ten jest zgodny z terminami przechowywania dokumentów finansowych na podstawie przepisów ustawy o rachunkowości. Należy też zauważyć, iż przepisy prawa stanowią o krótkich terminach na przekazanie informacji o zarejestrowanych transakcjach przez instytucje obowiązane Generalnemu Inspektorowi Informacji Finansowej.[344]

Do grupy pytań dotyczących działalności sektora finansowego należy zaliczyć też te, które **dotyczyły możliwości gromadzenia danych osobowych w związku z dopiero przewidywanym** - na dzień ich przedłożenia tych pytań Generalnemu Inspektorowi – **powstaniem obowiązku realizacji postanowień Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, oraz towarzyszących Uzgodnień Końcowych, podpisanych dnia 7 października 2014 r. w Warszawie**[345].

---

[343] Por. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz. Autor : Hara Michał, Kierzynka Rafał, Kołodziejski Paweł, LexisNexis, 2013.

[344] Zgodnie z art. 12 ust. 2 pkt 2 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, informacje o transakcjach zarejestrowanych zgodnie z art. 8 ust. 1 i 3, zawierające dane określone w ust. 1, przekazuje się do Generalnego Inspektora: 1) w terminie 14 dni po upływie każdego miesiąca kalendarzowego - w przypadku transakcji, o których mowa w art. 8 ust. 1; 2) niezwłocznie - w przypadku transakcji, o których mowa w art. 8 ust. 3.

[345] Mocą ustawy z dnia 20 marca 2015 r. o ratyfikacji Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA, oraz towarzyszących Uzgodnień Końcowych, podpisanych dnia 7 października 2014 r. w Warszawie (Dz. U 2015 r. poz 686) Prezydent RP uzyskał zgodę na jej ratyfikację.

Zarówno Związek Banków Polskich[346], jak i poszczególne banki[347] podnosiły w swych wystąpieniach, ich zdaniem uzasadniające rozpoczęcie gromadzenia danych osobowych klientów banków okoliczności mające uzasadnić istnienie podstaw prawnych takiego przetwarzania danych. Podmioty te doszukiwały się przesłanek legalności swych działań, np. w możliwości pozyskania zgód osób, których dane dotyczą na ich przetwarzanie, czy wręcz realizacji prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, bowiem takie przetwarzanie – zdaniem wnioskujących – nie narusza praw i wolności osób, których dane dotyczą.

W odpowiedziach GIODO konsekwentnie podnosił, iż dla działalności bankowej, podstawę przetwarzania przez bank danych osobowych jego klientów w pierwszej kolejności powinien stanowić przepis prawa. Tytułem przykładu, ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu określa zasady stosowania szczególnych środków ograniczających przeciwko osobom, grupom i podmiotom oraz obowiązki podmiotów uczestniczących w obrocie finansowym w zakresie gromadzenia i przekazywania informacji.

Zdaniem organu do spraw ochrony danych osobowych pozyskiwanie danych osobowych na podstawie zgody osób, których te dane dotyczą, nie jest w przedmiotowej sprawie właściwym. Zgoda na przetwarzanie danych osobowych powinna być bowiem udzielana dobrowolnie. Odbieranie zgody na pewno nie może być uznane za dobrowolne, gdy świadczenie usługi jest uzależnione od jej udzielenia. Tym samym umieszczenie klauzuli zgody np. w treści regulaminu działania określonego podmiotu – jako jednego z jej paragrafów – może prowadzić w konsekwencji do braku swobody jej wyrażenia przez tę osobę. Osoba ta bowiem może nie godzić się na uzależnienie swego działania w określonym celu, od wyrażenia zgody na przetwarzanie dotyczących jej danych osobowych w celach innych, co należy podkreślić w przedmiotowej sprawie - przed ratyfikowaniem stosownej umowy międzynarodowej w sprawie FATCA - określonych (narzuconych) przez administratora danych.

Generalny Inspektor wyjaśnił też, iż zgodnie z art. 7 pkt 5 ustawy o ochronie danych osobowych, przez zgodę osoby, której dane dotyczą rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, zgoda może być odwołana w każdym czasie.

---

[346] DOLiS-035-3549/14.
[347] DOLiS-035-1120/14, DOLiS-105/14.

Zgoda nie powinna mieć charakteru abstrakcyjnego, nie może dotyczyć przetwarzania danych osobowych „w ogóle", czy „na zapas". Chodzi o to, by zgoda odnosiła się do skonkretyzowanego stanu faktycznego, obejmowała tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania[348].

Co więcej, nawet w sytuacji pozyskania przez bank „dobrowolnej" zgody, duże wątpliwości może wywoływać jej prawidłowość także dlatego, iż pozycja dominująca, czy co najmniej brak równowagi w relacjach bank – klient, jest na rynku usług finansowych ciągle widoczna.

Dopiero dla sytuacji, w której podstawą prawną przetwarzania danych osobowych będą postanowienia ratyfikowanej umowy międzynarodowej, ewentualnie ujęte też w aktach prawa o randze ustawy, stanowiąc – zgodnie z art. 87 Konstytucji RP źródło powszechnie obowiązującego prawa Rzeczypospolitej Polskiej, spełniona będzie przesłanka legalności przetwarzania danych.

8.1.4. Służba zdrowia.

Jedno z zapytań pochodzących dotyczyło **dopuszczalności przekazywania informacji Policji przez szpitale dotyczących małoletnich pacjentów trafiających do szpitalnego oddziału ratunkowego** w sytuacjach zagrożenia zdrowia i zdarzeń takich, jak np.: próby samobójcze, stan po zażyciu farmaceutyków ogólnie dostępnych, m.in. w aptekach, po spożyciu alkoholu itp[349].

W odpowiedzi na wstępie zauważono, iż ustawa o ochronie danych osobowych określa ogólne zasady przetwarzania i ochrony danych osobowych, zaś skonkretyzowanie tychże zasad ma miejsce w szczególnych wobec jej regulacji przepisach prawa. Dlatego, jeżeli dla określonych sytuacji istnieją szczególne przepisy prawa regulujące przetwarzanie danych osobowych (w tym ich udostępnianie), to stosuje się je w pierwszej kolejności.

Ze względu na szczególny charakter kategorii danych, do jakiej należą dane o stanie zdrowia ustawa o ochronie danych osobowych zapewnia wysoki reżim ich ochrony. 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

[348] Por. J. Barta. P. Fajgielski, R. Markiewicz, *Ochrona Danych Osobowych. Komentarz,* Zakamycze 2004, s. 420.
[349] DOLiS-035-2732/14.

podstawę dla przetwarzania danych sensytywnych miałby stanowić przepis ustawy musiałby on także stwarzać pełne gwarancje ich ochrony[350].

Omawiając to zagadnienie Generalny Inspektor odwołał się do przepisów regulujących tajemnicę medyczną. Generalną zasadą jest utrzymywanie informacji związanych z pacjentem w tajemnicy i nieudostępnianie ich osobom trzecim. Tajemnicą objęte są informacje związane z pacjentem, w szczególności z jego stanem zdrowia, które zostały uzyskane przez personel medyczny w związku z wykonywaniem zawodu medycznego. Tym samym poufne są zarówno ujawnione w związku z udzielaniem świadczenia zdrowotnego informacje związane bezpośrednio z życiem osobistym, zawodowym czy publicznym pacjenta, jak i dane ustalone przez osoby wykonujące zawód medyczny w trakcie czynności zawodowych, np. wyniki przeprowadzonych badań, diagnoza, itp. Bez znaczenia dla obowiązku zachowania tajemnicy jest także to, czy lekarz powziął daną informację bezpośrednio od pacjenta, czy też osoby trzeciej, a nawet fakt uzyskania pewnych wiadomości wbrew woli pacjenta. Nie są natomiast chronione tajemnicą fakty i okoliczności powszechnie znane, nawet jeśli lekarz lub inna osoba wykonująca zawód medyczny, którzy nie wiedzieli o nich wcześniej, dowiedzieli się o nich właśnie w związku z wykonywaniem swojego zawodu.

Obowiązek taki nakłada na osoby wykonujące zawód medyczny art. 13 i art. 14 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.). Przepisy te stanowią, że pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego[351].

W zakresie ustawy o ochronie zdrowia psychicznego Generalny Inspektor wskazał, iż art. 50 ust. 1 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 2001 Nr 231 poz. 1375 za zm.) stanowi, że osoby wykonujące czynności wynikające z niniejszej ustawy są obowiązane do zachowania w tajemnicy wszystkiego, o czym powezmą

[350] 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.

[351] Zgodnie z art. 14 w celu realizacji prawa, o którym mowa w art. 13, osoby wykonujące zawód medyczny są obowiązane zachować w tajemnicy informacje związane z pacjentem, w szczególności ze stanem zdrowia pacjenta. Ustęp 2 powołanego przepisu określając zamknięty katalog wyjątków od powyższej zasady stanowi, że ust. 1 nie stosuje się, w przypadku gdy: 1) tak stanowią przepisy odrębnych ustaw; 2) zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób; 3) pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy; 4) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń.

wiadomość w związku z wykonywaniem tych czynności, stosownie do odrębnych przepisów, a nadto z zachowaniem przepisów niniejszego rozdziału. Jednakże zgodnie z art. 50 ust. 2 pkt 4 i 5, od obowiązku zachowania tajemnicy osoby wykonujące czynności wynikające z niniejszej ustawy są zwolnione m.in. w stosunku do Policji, policjanta upoważnionego pisemnie przez kierownika jednostki organizacyjnej Policji, prowadzącego czynności operacyjno-rozpoznawcze w zakresie poszukiwań i identyfikacji osób[352].

Obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu wynika również z przepisów ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2015 r. poz. 464 z późn. zm.), jakkolwiek, w przepisach tej ustawy dopuszczono ściśle określone wyjątki[353].

Wzajemny stosunek przepisów ustawy o ochronie danych osobowych i wyżej powołanych regulacji należy oceniać na gruncie art. 5 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem, jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z ustawy o ochronie danych osobowych, stosuje się przepisy tych ustaw. Przepisami „przewidującymi dalej idącą ochronę" w przedstawionej sprawie, w zakresie udostępniania danych, będą powołane wyżej przepisy dotyczące szeroko pojmowanej tajemnicy medycznej.

W innym pytaniu z zakresu dotyczącego przetwarzania danych o stanie zdrowia podniesiono z kolei wątpliwości w zakresie **udostępnienia przez lekarza ginekologa**

---

[352] Zgodnie z art. 50 ust. 2 ustawy o ochronie zdrowia psychicznego 2. Od obowiązku zachowania tajemnicy osoba wymieniona w ust. 1 jest zwolniona w stosunku do: 1) lekarza sprawującego opiekę nad osobą z zaburzeniami psychicznymi; 2) właściwych organów administracji rządowej lub samorządowej co do okoliczności, których ujawnienie jest niezbędne do wykonywania zadań z zakresu pomocy społecznej; 3) osób współuczestniczących w wykonywaniu czynności w ramach pomocy społecznej, w zakresie, w jakim to jest niezbędne; 4) Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Agencji Wywiadu, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Policji, Żandarmerii Wojskowej, Straży Granicznej, Służby Więziennej, Biura Ochrony Rządu i ich upoważnionych pisemnie funkcjonariuszy lub żołnierzy w zakresie niezbędnym do przeprowadzenia postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych; 5) policjanta, upoważnionego pisemnie przez kierownika jednostki organizacyjnej Policji, prowadzącego czynności operacyjno-rozpoznawcze w zakresie poszukiwań i identyfikacji osób.

[353] Art. 40 ust. 1 ustawy o zawodach lekarza i lekarza dentysty stanowi, że lekarz ma obowiązek zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu. Przepisu ust. 1 nie stosuje się, gdy: 1) tak stanowią ustawy; 2) badanie lekarskie zostało przeprowadzone na żądanie uprawnionych, na podstawie odrębnych ustaw, organów i instytucji; wówczas lekarz jest obowiązany poinformować o stanie zdrowia pacjenta wyłącznie te organy i instytucje; 3) zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób; 4) pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, po uprzednim poinformowaniu o niekorzystnych dla pacjenta skutkach jej ujawnienia; 5) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie lekarzowi sądowemu; 6) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innemu lekarzowi lub uprawionym osobom uczestniczącym w udzielaniu tych świadczeń. Stosownie do ust. 2a cytowanego artykułu w sytuacjach, o których mowa w ust. 2, ujawnienie tajemnicy może nastąpić wyłącznie w niezbędnym zakresie.

prowadzącego ciążę danych medycznych Zakładowi Ubezpieczeń Społecznych, w związku z postępowaniem wyjaśniającym w sprawie obowiązku ubezpieczenia oraz uprawnienia do świadczeń[354].

W sprawie tej poinformowano, iż przepisu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta o obowiązku zachowania tajemnicy medycznej nie stosuje się w przypadku, gdy tak stanowią przepisy odrębnych ustaw. Zgodnie natomiast z przepisami ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (t.j. Dz. U. z 2014 r. poz. 159), w celu kontroli lekarz orzecznik Zakładu Ubezpieczeń Społecznych może zażądać od wystawiającego zaświadczenie lekarskie udostępnienia dokumentacji medycznej dotyczącej ubezpieczonego stanowiącej podstawę wydania zaświadczenia lekarskiego lub udzielenia wyjaśnień i informacji w sprawie[355].

W przedmiocie zaś wątpliwości osoby pytającej odnośnie tego, iż „o dane nie zwraca się (...) kierownik wydziału Ubezpieczeń i składek (...)", GIODO wskazał, iż do zakresu działania Zakładu Ubezpieczeń Społecznych należy między innymi realizacja przepisów o ubezpieczeniach społecznych, w tym stwierdzanie i ustalanie obowiązku ubezpieczeń społecznych, ustalanie uprawnień do świadczeń z ubezpieczeń społecznych oraz wypłacanie tych świadczeń, chyba że na mocy odrębnych przepisów obowiązki te wykonują płatnicy składek, czy orzekanie przez lekarzy orzeczników Zakładu oraz komisje lekarskie Zakładu dla potrzeb ustalania uprawnień do świadczeń z ubezpieczeń społecznych[356].

Kolejne pytanie - wystosowane przez Głównego Inspektora Farmaceutycznego - dotyczyło **przesyłania przez apteki ogólnodostępne kserokopii lub skanów recept do firm trudniących się obrotem produktami leczniczymi, tj. podmiotów odpowiedzialnych i hurtowni farmaceutycznych**[357].

W odpowiedzi wskazano pytającemu, iż obrót produktami leczniczymi, w tym zasady i tryb przyjmowania i wydawania tych produktów określony jest przepisami prawa, w szczególności ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne (t.j. Dz. U. z 2008 r. Nr 45 poz. 271 z poźn. zm.), oraz wydanym na jej podstawie rozporządzeniu Ministra Zdrowia z dnia 26 lipca 2002 r. w sprawie procedur Dobrej Praktyki Dystrybucyjnej (tekst

---

[354] DOLiS-035-448/14

[355] Art. 59 ust. 3 pkt 3 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.

[356] Zgodnie z art. 68 ust. 1 pkt 1a i 1b i 1f ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t.j. Dz.U.2015 r. poz. 121).

[357] Sprawa GIODO o sygn.: DOLiS-035-2229/14, pismo GIF z dnia 18 września 2014 r. o sygn.: GIF-N-076/74-1/MP/14.

pierwotny: Dz. U. z 2002 r. Nr 144 poz. 1216). Przepisy te stanowią, iż obrót produktami leczniczymi może być prowadzony tylko na zasadach określonych w ustawie[358]. Przepisy zaś ustawy Prawo Farmaceutyczne, czy rozporządzenia Ministra Zdrowia w sprawie procedur Dobrej Praktyki Dystrybucyjnej, stanowią przepisy szczególne, wobec uregulowań ustawy o ochronie danych osobowych, i powinny być stosowane w pierwszej kolejności.

Zgodnie z § 7 rozporządzenia w sprawie procedur Dobrej Praktyki Dystrybucyjnej, hurtownie farmaceutyczne prowadzi się z uwzględnieniem procedur m.in. w zakresie czynności należących do pracownika przyjmującego i wydającego produkty lecznicze oraz zasad i trybu sporządzania protokołu przyjęcia lub wydania produktów leczniczych, których to minimalne wymagania ujęte są w § 8 – i brak jest w tych przepisach unormowań dotyczących kwestionowanej praktyki. Podkreślono też, iż ww. procedury nie mogą swymi postanowieniami zmieniać (rozszerzać) postanowień ustawowych. Jednoznacznie zaś przepisy ustawy Prawo farmaceutyczne określają możliwość cofnięcia zezwolenia na prowadzenie apteki ogólnodostępnej, m.in. gdy apteka przekazuje, z wyłączeniem Inspekcji Farmaceutycznej i Narodowego Funduszu Zdrowia, dane umożliwiające identyfikację indywidualnego pacjenta, lekarza lub świadczeniodawcy[359].

8.1.5. Zatrudnienie.

Ciekawe zagadnienie w tej materii zostało podniesione przez Kancelarię Prezesa Rady Ministrów, w związku powstaniem wątpliwości **w jaki sposób ma nastąpić weryfikacja kandydatów do pracy w służbie cywilnej pod względem obywatelstwa**[360]. Zgodnie bowiem z przepisami ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (tekst pierwotny: Dz. U. z 2008 r. Nr 227, poz. 1505 z późn. zm.), w służbie cywilnej może być zatrudniona osoba, która jest obywatelem polskim[361], z pewnymi zastrzeżeniami. W szczególności wątpliwym było, czy od obywateli Unii Europejskiej oraz obywateli innych państw, którym na podstawie umów międzynarodowych lub przepisów prawa wspólnotowego przysługuje

[358] Zgodnie z art. 65 ustawy Prawo farmaceutyczne.
[359] Art. 103 ustawy Prawo farmaceutyczne.
[360] DOLiS-035-1487/14.
[361] Zgodnie z art. 4, w służbie cywilnej może być zatrudniona osoba, która: 1) jest obywatelem polskim, z zastrzeżeniem art. 5; 2) korzysta z pełni praw publicznych; 3) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 4) posiada kwalifikacje wymagane na dane stanowisko pracy; 5) cieszy się nieposzlakowaną opinią. Artykuł 5 ust. 1 tej samej ustawy stanowi, iż . dyrektor generalny urzędu, upowszechniając informacje o wolnych stanowiskach pracy, wskazuje, za zgodą Szefa Służby Cywilnej, stanowiska, o które, poza obywatelami polskimi, mogą ubiegać się obywatele Unii Europejskiej oraz obywatele innych państw, którym na podstawie umów międzynarodowych lub przepisów prawa wspólnotowego przysługuje prawo podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej.

prawo podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej można żądać, ewentualnie można tym osobom pozwolić na złożenie kopii dokumentów potwierdzających ich obywatelstwo.

W odpowiedzi zauważono, iż ustawa o służbie cywilnej i akty wykonawcze do tej ustawy zawierają precyzyjne regulacje zobowiązujące kandydatów na (wybrane) wolne stanowiska w służbie cywilnej do przedstawienia określonych rodzajów dokumentów potwierdzających wypełnienie wymaganych tą ustawą warunków. Tytułem przykładu, są to rozporządzenie Prezesa Rady Ministrów z dnia 23 kwietnia 2009 r. w sprawie rodzajów dokumentów potwierdzających znajomość języka polskiego przez osoby nieposiadające obywatelstwa polskiego, ubiegające się o zatrudnienie w służbie cywilnej.

Pytającemu także wskazano, iż do podnoszonej sprawy znajdują zastosowanie uregulowania art. 22^1 § 3 i 4 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2014 r. poz. 1502 z późn. zm.). Zgodnie bowiem z art. 22^1 § 4 tego aktu prawnego, pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Z kolei zgodnie z § 3 ww. artykułu, udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą, jakkolwiek pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i 2.

Tym samym, wolą ustawodawcy, którego racjonalność należy domniemywać aby „wiodącą" formą udostępnienia informacji – danych osobowych – przez kandydata do pracy było przyszłemu pracodawcy jest oświadczenie. Dopiero natomiast w przypadku wątpliwości dotyczących ujętych w oświadczeniu informacji pracodawca ma prawo żądać ich udokumentowania, lub też wyłącznie wglądu do dokumentów potwierdzających treść oświadczenia.

Odnośnie tematów związanych z zatrudnieniem, wartym w tym miejscu wspomnienia jest sprawa, w której pytający zwrócił się do organu do spraw ochrony danych osobowych w związku z trudnościami, jakie napotkał u swego pracodawcy odnośnie **realizacji jego prawa wglądu do dotyczącej go dokumentacji pracowniczej**, w szczególności odnośnie ustalania wynagrodzenia[362].

[362] DOLiS-035-1060/14.

W odpowiedzi Generalny Inspektor wskazał na podstawy prawne wglądu do akt pracowniczych, powołując przepisy Kodeksu pracy dotyczące obowiązków pracodawcy w zakresie prowadzenia dokumentacji płacowej.

Pracodawca jest obowiązany terminowo i prawidłowo wypłacać wynagrodzenie oraz prowadzić dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników. Obowiązek prawidłowego i terminowego wypłacania wynagrodzenia za pracę odnosi się także do wypłaty innych świadczeń przysługujących pracownikowi, w tym diet[363]. Istotnym jest, iż pracodawca, na żądanie pracownika, jest obowiązany udostępnić mu do wglądu dokumenty, na podstawie których zostało obliczone jego wynagrodzenie, o czym konkretnie stanowi przepis prawa[364].

W kwestii natomiast tego, **czy pracodawca może przekazywać pasek wynagrodzeń oraz comiesięczny odcinek RMUA swoim pracownikom poprzez innych pracowników, oraz czy może bez zgody pracownika przekazać jego CV innym pracownikom, którzy go o to poproszą**[365], Generalny Inspektor wyjaśnił, że pracodawca (osoba, która wykonuje za pracodawcę czynności z zakresu stosunku pracy) nie może udostępniać danych pracownika osobom nieupoważnionym. Nieuzasadnione udostępnienie informacji o pracowniku innym pracownikom może bowiem stanowić naruszenie dóbr osobistych zatrudnionego oraz prawa do ochrony jego danych osobowych. Pracodawca wykonując swoje obowiązki związane z nawiązywaniem lub realizowaniem umowy o pracę jest związany przepisami prawa. Stanowią je przede wszystkim przepisy prawa pracy zawarte głównie w Kodeksie pracy oraz innych ustawach i aktach wykonawczych dotyczących stosunku pracy. Przepisy Kodeksu pracy określają m.in. zakres danych jakie może pozyskiwać pracodawca zarówno od kandydata do pracy, jak i pracownika. Przepisy prawa nie przewidują natomiast uprawnienia pracodawcy do przekazywania danych pracownika innym pracownikom, gdy brak jest ku temu uzasadnienia. Podkreślenia wymaga także, że jednym z podstawowych obowiązków pracodawcy zaliczanych do zasad prawa pracy jest poszanowanie godności oraz prywatności pracownika jako jego dóbr osobistych, zgodnie z art. 11^1 Kodeksu pracy. Naruszenie tego obowiązku może być podstawą uzasadnionych roszczeń pracownika, w tym rozwiązania przez niego umowy o pracę bez wypowiedzenia na podstawie art. 55 § 1^1 Kodeksu pracy.

[363] Art. 94, art. 282 § 1 Kodeksu pracy.
[364] Art. 85 § 5 Kodeksu pracy.
[365] DOLiS-035-1370/14.

Stąd informacje dotyczące poszczególnych pracowników mogą być dostępne jedynie dla ograniczonego kręgu osób u danego pracodawcy, w jasno określonych ustawowo celach. - Do osób takich należą najczęściej osoby zarządzające, w imieniu pracodawcy, zakładem pracy, przełożeni danego pracownika, osoby prowadzące sprawy osobowe, zatrudnienia i płac, radcy prawni świadczący dla pracodawcy pomoc prawną, czy też przedstawiciel związku zawodowego, do którego to związku dany pracownik należy lub - w przypadku pracownika niezrzeszonego - związku który podjął się obrony i interesów pracownika (art. 7 ustawy o związkach zawodowych). Osoby te w ramach wykonywanych obowiązków są najczęściej upoważnione do przetwarzania danych innych pracowników ponieważ wiąże się to ściśle z zakresem zadań, jakie wykonują one w danym zakładzie pracy. Są one - zgodnie z art. 39 ustawy o ochronie danych osobowych - obowiązane zachowywać dane osobowe w poufności.

W związku z wątpliwościami interpretacyjnymi, jakie pojawiły się podczas kontroli prowadzonej w jednym z podmiotów województwa małopolskiego przez inspektora pracy jednego z Okręgowych Inspektoratów Pracy, poprosił on GIODO o zajęcie stanowiska, **czy w świetle wymogów ustawy o ochronie danych osobowych, informacje dotyczące usprawiedliwionych, bądź też nieusprawiedliwionych nieobecności w pracy mogą być zamieszczane na zbiorczej liście obecności wraz z podpisami innych obecnych w danym dniu pracowników danego podmiotu**[366].

Omawiając powyższe wątpliwości Generalny Inspektor wskazał, iż w świetle art. 149 Kodeksu pracy na każdym pracodawcy, niezależnie od liczby zatrudnianych pracowników, ciąży obowiązek prowadzenia ewidencji czasu pracy. Jest to konieczne w celu prawidłowego ustalenia wynagrodzenia oraz innych świadczeń przysługujących pracownikowi ze stosunku pracy. Kodeks pracy nie narzuca jednak sposobu potwierdzania obecności w pracy przez pracodawcę. Niemniej każdy pracodawca, bez względu na wielkość i liczbę zatrudnionych osób, ma obowiązek określenia sposobu potwierdzania obecności. W firmach zatrudniających co najmniej 20 pracowników zagadnienia związane z organizacją i porządkiem określa regulamin pracy. Według art. 104^1 § 1 Kodeksu pracy regulamin musi określać przyjęty u danego pracodawcy sposób potwierdzania przez zatrudnionych przybycia i obecności oraz usprawiedliwiania nieobecności w pracy. Pracodawcy, którzy nie mają obowiązku wydania regulaminu, muszą, zgodnie z art. 29 § 3 pkt 5 Kustawa ochro.p., poinformować każdego

[366] DOLiS-035-922/14.

nowo zatrudnionego m.in. o przyjętym sposobie potwierdzania przybycia i obecności w pracy oraz usprawiedliwiania nieobecności. Informacja na ten temat musi być przekazana w ciągu siedmiu dni od dnia zawarcia umowy o pracę.

Rozwiązanie, zgodnie z którym zbiorcze listy obecności prowadzone są w ten sposób, - że pracownicy potwierdzają swoją obecność jedynie na kartach niezawierających informacji na temat nieobecności w pracy należy uznać za przykład bardzo starannej i godnej naśladowania dbałości o poszanowanie prywatności pracownika i jego prawa do ochrony danych osobowych.

8.1.6. Mieszkalnictwo.

Do Biura GIODO wpłynęło zapytanie wspólnoty mieszkaniowej, w którym poproszono o opinię, **czy zasadnym jest żądanie wspólnoty mieszkaniowej skierowane do Zakładu Gospodarowania Nieruchomościami jednej z gmin, przekazania wspólnocie danych osobowych najemców/użytkowników lokali komunalnych znajdujących się w budynku wspólnoty mieszkaniowej**[367]. Jako podstawę prawną tego żądania wskazano przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 16 sierpnia 1999 r. w sprawie warunków technicznych użytkowania budynków mieszkalnych (Dz. U. z 1999 r. Nr 74 poz. 836 z późn. zm.).

W odpowiedzi wskazano, iż zgodnie z § 3 pkt 5 powołanego powyżej rozporządzenia, użyte w rozporządzeniu określenie dokumentacja użytkowania oznacza - dokumentację odbioru budynku wraz z m.in. książką obiektu budowlanego, kopiami imiennych przydziałów lokali i umowami najmu lokali.

Wątpliwym jednak pozostaje, czy w sytuacji, gdy określone lokale, do których prawo własności posiada wspólnota mieszkaniowa znajdują się we władaniu innego podmiotu w związku z umową wiążącą wspólnotę z tym podmiotem, dokumentacja powinna obejmować także np. kopie imiennych przydziałów lokali, czy umowy najmu lokali, które stanowią o stosunkach prawnych łączących ww. podmiot z osobami użytkującymi lokale.

Zdaniem organu do spraw ochrony danych osobowych, wystarczającym jest – co do zasady – ujęcie w dokumentacji, o której mowa w § 3 pkt 5 rozporządzenia, np. kopii umowy łączącej wspólnotę z podmiotem faktycznie dysponującym lokalami, tj. Zakładem Gospodarowania Nieruchomościami, nie zaś np. umów łączących ten podmiot z ich użytkownikami.

[367] DOLiS-035-3608/14.

Danych osobowych nie należy zbierać bez podstawy prawnej i niejako „na zapas", a z taką sytuacją możemy mieć do czynienia np., gdy wspólnota mieszkaniowa będzie pozyskiwać dane osobowe użytkowników lokali w każdym przypadku, uzasadniając to koniecznością bliżej nieokreślonego „zapewnieniem bezpieczeństwa ludzi i mienia", czy ochroną „uzasadnionych interesów osób trzecich" – jak wskazała wspólnota mieszkaniowa.

Podnieść jednak należy, iż mogą zaistnieć konkretne sytuacje, w której przetworzenie danych osobowych użytkownika lokal będzie wspólnocie niezbędne, np. w związku z koniecznością dokonania napraw w lokalu.

Odpowiadając z kolei na pytanie dotyczące legalności **udostępnienia przez zarządcę na wniosek każdego właściciela lokalu, który określi cel otrzymania tych danych, przekazania danych dotyczące innych członków wspólnoty mieszkaniowej**, tj. adresu do korespondencji, telefonu, adresu e-mail, które są przekazane administratorowi danych tylko w celach kontaktu pomiędzy administratorem a właścicielem w przypadku awarii lub innych zdarzeń[368], GIODO wyjaśnił, iż tworzone i działające na podstawach przepisów ustawy z dnia 24 czerwca 2000 r. o własności lokali (Dz. U. Nr 80, poz. 903 z późn. zm.) wspólnoty mieszkaniowe, w zakresie nieuregulowanym wyżej wymienionym aktem prawnym są obowiązane działać na podstawie innych przepisów prawa, w tym ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2014 r. poz. 121 z późn. zm.). Zgodnie natomiast z art. 200 Kodeksu cywilnego, 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. Dane udostępniane członkowi wspólnoty powinny być przez niego przetwarzane zgodnie z celem udostępnienia. Nie jest więc dopuszczalne udostępnienie współwłaścicielom określonej nieruchomości danych, których przetwarzanie nie jest niezbędne do współdziałania w zarządzie nieruchomością wspólną oraz do sprawowania kontroli działalności jej zarządcy. Zakres zaś udostępnianych danych osobowych należy niejako dostosować do potrzeb indywidualnych sytuacji. Wysoce bowiem wątpliwym jest, aby wszystkie dane osobowe, o których mowa na wstępie omówienia tego zagadnienia były potrzebne członkowi wspólnoty w każdej sytuacji mającej związek z koniecznością podjęcia działań zarządu nieruchomością wspólną.

[368] DOLiS-035-3551/14.

Kolejnym, istotnym zagadnieniem z którym w swej działalności spotkał się Generalny Inspektor Ochrony Danych Osobowych, była **kwestia uprawnień rady nadzorczej spółdzielni do przetwarzania danych osobowych ujętych w umowach zawieranych przez spółdzielnię, w tym umowach o pracę**, w ramach czynności kontrolnych[369].

GIODO przypomniał, iż przetwarzając dane osobowe w sposób opisany w przepisach ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (t. j. Dz. U. z 2013 r. poz. 1222 z późn. zm.), a w zakresie nieuregulowanym w tych przepisach – ustawy z dnia 16 września 1982 r. Prawo spółdzielcze (t. j. Dz. U. z 2013 r. poz. 1443 z późn. zm.), spółdzielnia korzysta z przesłanki wskazanej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, zgodnie z którą przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Kwestię dopuszczalności udostępnienia radzie nadzorczej informacji regulują przepisy ustawy o spółdzielniach mieszkaniowych, a w zakresie nieuregulowanym w tych przepisach – ustawy Prawo spółdzielcze, a także postanowienia statutu spółdzielni – albowiem zgodnie z art. 46 § 2 ustawy Prawo spółdzielcze „statut może zastrzec do zakresu działania rady jeszcze inne uprawnienia" - w szczególności określenie regulaminu rady nadzorczej. Należy jednak mieć na uwadze fakt, iż postanowienia statutu, czy uchwały spółdzielni, nie mogą pozostawać w sprzeczności z powszechnie obowiązującym prawem.

W myśl art. 46 § 1 pkt 2 Prawa spółdzielczego, do zakresu działania rady należy nadzór i kontrola działalności spółdzielni. W celu wykonania swoich zadań rada może żądać od zarządu, członków i pracowników spółdzielni wszelkich sprawozdań i wyjaśnień, przeglądać księgi i dokumenty oraz sprawdzać bezpośrednio stan majątku spółdzielni (art. 46 § 4 cytowanej ustawy). Powołane przepisy nie określają wprost do jakiego rodzaju informacji i jakich dokumentów mogą mieć dostęp członkowie rady nadzorczej w związku z dokonywaniem swoich czynności. Wszelkie zatem czynności związane z przeprowadzaniem np. kontroli przez radę nadzorczą, w tym możliwość zapoznania się jej członków z określonymi informacjami, może odbywać się jedynie na podstawie interpretacji wskazanych wyżej przepisów.

Udostępnianie radzie nadzorczej jakiejkolwiek informacji powinno być determinowane zakresem przeprowadzanej kontroli i nie wykraczać poza jej ramy. Jednakże, trzeba mieć na

[369] DOLiS-3606/14.

uwadze fakt, iż administrator danych, który decyduje o celach i środkach przetwarzania danych osobowych, dokonujący na danych osobowych jakichkolwiek operacji 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 (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Oznacza to, że administrator nie może przetwarzać (udostępniać) danych w zakresie szerszym niż niezbędny dla osiągnięcia określonego celu, jak też danych o większym stopniu szczegółowości, wykraczającym poza ten cel. Udostępnianie danych w zbyt szerokim zakresie może prowadzić do naruszenia przepisów ustawy o ochronie danych osobowych. Dlatego też rada nadzorcza powinna mieć dostęp do akt zawierających dane osobowe jedynie w zakresie niezbędnym ze względu na cel i przedmiot kontroli.

Generalny Inspektor zauważył też, iż zgodnie z art. 8^1 ust. 1 ustawy o spółdzielniach mieszkaniowych członek spółdzielni mieszkaniowej ma prawo otrzymania odpisu statutu i regulaminów oraz kopii uchwał spółdzielni i protokołów obrad spółdzielni, protokołów lustracji, rocznych sprawozdań finansowych oraz faktur i umów zawieranych przez spółdzielnię z osobami trzecimi.

Gdy istnieje podjęta z mocy prawa uchwała zawierająca w swojej treści informacje o wysokości wynagrodzenia otrzymywanego przez ww. osoby, to dopuszczalne jest udostępnienie tych informacji w treści takiej uchwały na podstawie wyżej powołanego art. 8^1 ust. 1 ustawy o spółdzielniach mieszkaniowych. Podobnie, jeżeli statut spółdzielni przewiduje udostępnienie informacji na zasadach w nim określonych.

8.1.7. Internet i Telekomunikacja.

Nadal wiele zapytań wpływających do Biura GIODO dotyczy zagadnień związanych użytkowaniem sieci Internet. W szczególności **wielu użytkowników tej sieci ma wątpliwości dotyczące umieszczania na komputerach osobistych plików cookies**[370].

W jednej z takich spraw wyjaśniono pytającemu, że kwestia dotycząca plików cookies uregulowana została w przepisach ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243 z późn. zm.). Zgodnie z przepisami Prawa telekomunikacyjnego przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego jest

[370] DOLiS-035-379/14.

dozwolone, pod określonymi w tym artykule warunkami, tj.: 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. Wyrażenie zaś zgody, o której mowa powyżej może zaś nastąpić za pomocą ustawień oprogramowania zainstalowanego w wykorzystywanym przez niego telekomunikacyjnym urządzeniu końcowym lub konfiguracji usługi[371].

Istnieje też możliwość odstąpienia od powyższych warunków w (najczęściej) komputerze czy telefonie użytkownika, jeżeli przechowywanie lub uzyskanie dostępu do informacji jest konieczne do: 1) wykonania transmisji komunikatu za pośrednictwem publicznej sieci telekomunikacyjnej; 2) dostarczania usługi telekomunikacyjnej lub usługi świadczonej drogą elektroniczną, żądanej przez abonenta lub użytkownika końcowego.

Zgodnie z przepisami Prawa telekomunikacyjnego 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, 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

[371] Artykuł 173 Prawa telekomunikacyjnego.

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.

Należy jednak zaznaczyć, iż to Prezes Urzędu Komunikacji Elektronicznej jest organem regulacyjnym w zakresie działalności pocztowej, telekomunikacyjnej i gospodarki częstotliwościowej oraz kontroli spełniania wymagań dotyczących kompatybilności elektromagnetycznej. Powyższe zaś informacje, przedstawiono pomocniczo, jako pozostające niejako „na styku" działalności Generalnego Inspektora i innego organu regulacyjnego regulatorów.

W odniesieniu do zagadnień związanych z usługami świadczonymi za pomocą Internetu, w sprawie dotyczącej aspektów **regulaminu „strefy kibica" i zakupów biletów online**[372] Generalny Inspektor wyjaśnił, iż zagadnienia związane z danymi o ruchu telekomunikacyjnym (tzw. logi systemowe serwerów i innych urządzeń sieciowych, które pośredniczą w realizacji połączenia) zawierającymi dane techniczne dotyczące połączeń (w tym numery IP) będą stanowiły informacje, które umożliwiają identyfikację osób, których dotyczą, natomiast same ich nie identyfikują. Podobnie jak numery telefonów, adresy IP identyfikujące urządzenia w sieci komputerowej (np. nr IP urządzeń w sieci Internet), nie zawsze będą przypisane przez operatorów do konkretnej osoby fizycznej. Dane te mogą być przypisane określonej firmie, organizacji lub w ogóle nieprzypisane żadnemu podmiotowi, jak np. adresy IP użytkowników podłączających się do niezabezpieczonych sieci bezprzewodowych (hotspotów).

Publiczny adres IP identyfikujący stację komputerową w sieci jest odpowiednikiem numeru telefonu, który przypisany jest do aparatu telefonicznego stanowiącego zakończenie linii telekomunikacyjnej. W obydwu przypadkach urządzenia te przypisane mogą być do konkretnej osoby fizycznej niezależnie od tego, w jaki sposób czynność ta technologicznie jest wykonana. Obydwa numery są unikalnymi w danej chwili w skali całego świata. Mając - na uwadze powyższą analogię należy rozgraniczyć dwie sytuacje.

Podobnie jak w przypadku przetwarzania danych na potrzeby telekomunikacji, w przypadku danych dotyczących publicznego numeru IP przypisanego komputerowi należy

[372] DOLiS-035-829/14

wyróżnić dwa rodzaje danych: dane o abonentach dostawców Internetu (Providerów Internetowych) zawierające numer publiczny IP w powiązaniu z danymi osobowymi abonenta (osoby prywatnej) lub danymi firmy; dane o ruchu telekomunikacyjnym, czyli dane na temat wykonywanych połączeń teleinformatycznych składających się między innymi z numerów IP, używanych protokołów oraz czasu trwania połączenia. Dane te podobnie jak dla telefonii nie zawierają wprost danych osobowych abonenta, a jedynie dane techniczne dotyczące wykonanych połączeń i rodzaju usług, z których abonent korzystał.

Dane o abonentach internetowych, porównane wcześniej do danych abonentów telefonicznych, znane są operatorowi będącym dostawcą Internetu. Posiadane przez operatora dane osobowe abonentów są danymi, które w pełni identyfikują osobę fizyczną. Nie są to dane, które jedynie umożliwiałyby ustalenie tożsamości osób, których dotyczą po wykonaniu dodatkowych działań. Są to dane osób już zidentyfikowanych.

Niejako na marginesie podkreślić należy, iż administrator danych osobowych jest zobowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane[373]. Ponadto wydaje się być zasadnym przyjęcie domniemania racjonalnego działania ustawodawcy, pozostawiającego administratorom danych swobodę wyboru środków koniecznych do spełnienia obowiązku określonego przepisem prawa w tym aspekcie. Intencją ustawodawcy wydaje się być także uwzględnienie sytuacji, w których zidentyfikowanie osób wprowadzających dane do systemów teleinformatycznych przez administratorów tych systemów nie jest dokonywane, chociażby z powodów racjonalnych, bądź też z powodu możliwości naruszenia takim przetwarzaniem art. 26 ust. 1 pkt. 3 ustawy. Kwestia uznania informacji za daną osobową jest zależna od charakteru, okoliczności, sposobu i celu, w jakim dane te są zbierane i wykorzystywane, zaś administratorzy danych i tak najczęściej będą posiadać informacje umożliwiające przyporządkowanie danych wprowadzonych do systemu określonej osobie, chociaż, informacje te nie pozwalają na ustalenie tożsamości tych osób. Tym samym, możliwa jest realizacja obowiązków dotyczących kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane niezależnie od tego, czy podane przez użytkownika systemu dane (bądź też usługobiorcę – w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną; Dz. U. z 2013 r., poz. 1422), identyfikujące tę osobę, są prawdziwe. Co więcej, wykładnia funkcjonalna przepisów ustawy

[373] Art. 38 ustawy o ochronie danych osobowych.

o ochronie danych osobowych oraz analiza przepisów ustawy o świadczeniu usług drogą elektroniczną wskazuje, że kontrola może być zapewniona także poprzez posługiwanie się przez administratorów systemów internetowych takimi informacjami o ich użytkownikach, jakimi dysponują. Kontrolowanie bowiem użytkownika dla którego znany jest jedynie jego pseudonim (nick), bądź adres poczty elektronicznej - obok informacji o terminach logowań, nr IP jego komputera itp. - i na podstawie takich właśnie informacji, należy uważać za realizację takiego obowiązku. Administratorzy danych zaś, na podstawie ustawy o świadczeniu usług drogą elektroniczną, nie mają obowiązku, dochodzić prawdziwości tych danych.

Odpowiadając z kolei na pytanie dotyczące **zbierania informacji o użytkownikach portalu Allegro.pl, tj. nicku użytkownika i historii zwieranych przez niego transakcji w aspekcie ewentualnego podlegania takiego procesu przepisom ustawy o ochronie danych osobowych**[374], Generalny Inspektor na wstępie wyjaśnił, iż (także) jeżeli chodzi o „Nick" (z ang. *nickname* - przezwisko, pseudonim) to jest to ciąg znaków tworzący nazwę pod jaką dana osoba chce występować, w przypadku gdy nie chce się ona posługiwać swoim imieniem lub/i nazwiskiem. Biorąc pod uwagę serwisy internetowe, np. portale społecznościowe, „nick" osoby często może być tożsamy z nazwą użytkownika, po której dana osoba jest identyfikowana. Pod pojęciem „nick" rozumie się również nazwę używaną do podpisania wiadomości umieszczanych na forach dyskusyjnych, podpisywania komentarzy zamieszczanych na portalach informacyjnych, oznaczania osób uczestniczących w czatach, czy też nazwę w komunikatorach internetowych. W zależności od rodzaju usługi, nazwa „nick" może mieć charakter tymczasowy użyty w czasie ad-hoc, np. na czacie dla potrzeb oznaczenia osoby na czas jej udziału w dyskusji, czy skomentowania wydarzenia w portalu informacyjnym lub stały, w przypadku użytkowników rejestrowanych na forach dyskusyjnych, w portalach społecznościowych, itp. Przy „nicku" stałym dla każdego połączenia się z daną usługą, ta sama osoba może występować pod tą samą nazwą. Przy „nicku" tymczasowym dla każdego połączenia się z daną usługą ta sama osoba może występować za każdym razem pod inną nazwą.

W każdym więc przypadku, niezależnie od rodzaju „nicku", system informatyczny lub serwis rejestruje numery IP komputerów, z których dokonywane są określone działania przez użytkownika. Nazwa („nick") przypisana konkretnemu użytkownikowi pełni zatem rolę

[374] DOLiS-035-312/14.

dodatkowej informacji ułatwiającej jego identyfikację. W określonych zatem sytuacjach, o ile nie wymagałoby to nadmiernych kosztów, czasu lub działań, „nick" może być uznany za dane osoby możliwej do zidentyfikowania. Dlatego, ocena, czy „Nick" pozwoli na jednoznaczne ustalenie tożsamości użytkownika, a tym samym, czy do tej danej osobowej będą miały zastosowanie przepisy ustawy o ochronie danych osobowych należy do podmiotu, który określonymi informacjami dysponuje. To on powinien ocenić, czy ewentualne koszty, czas lub działania zmierzające do bezbłędnego ustalenia tożsamości nie są nadmierne[375].

W związku z powyższym to, czy w konkretnym przypadku dostępne informacje o konkretnej osobie fizycznej będą danymi osobowymi, należy rozważyć indywidualnie.

Generalny Inspektor informował też o zakresie swych kompetencji i ich rozróżnieniu od kompetencji Urzędu Komunikacji Elektronicznej. Tytułem przykładu, w związku z jednym z pytań dotyczącym tego, **czy GIODO ma w zakresie swoich działań nadzór nad komunikacją elektroniczną w zakresie wymuszania przez strony internetowe instalowania na komputerach plików cookies**[376]. Generalny Inspektor wyjaśnił, iż to Prezes Urzędu Komunikacji Elektronicznej jest organem regulacyjnym w zakresie działalności pocztowej, telekomunikacyjnej i gospodarki częstotliwościowej oraz kontroli spełniania wymagań dotyczących kompatybilności elektromagnetycznej[377].

W kolejnej odpowiedzi Generalny Inspektor omówił kwestie związane **z umieszczaniem przez Urząd Komunikacji Elektronicznej w swoim oficjalnym wykazie kody pocztowe polskich radiowych nadawców indywidualnych**[378].

W tej sprawie GIODO wskazał, iż jeżeli szczególny przepis prawa nakłada na określony podmiot obowiązek udostępniania danych osobowych, udostępnienie w tym przedmiocie nie może być traktowane jako naruszenie przepisów ustawy o ochronie danych osobowych. W niniejszym przypadku przepisy takie zawarte są w ustawie Prawo telekomunikacyjne.

[375] W myśl art. 6 ust. 1 ustawy o ochronie danych osobowych 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, 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 takie 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.

[376] DOLiS-035-379/14.

[377] Zgodnie z art. 192 ustawy Prawo telekomunikacyjne.

[378] DOLiS-035-2066/14.

Zgodnie bowiem z art. 148a wyżej wskazanej ustawy Prezes UKE publikuje na stronie podmiotowej BIP UKE informacje o wydanych pozwoleniach, decyzjach o rezerwacji częstotliwości oraz decyzjach o zezwoleniu na czasowe używanie urządzeń radiowych, o których mowa w art. 144a oraz art. 144b, obejmujące: nazwę (firmę) podmiotu uprawnionego; zakres częstotliwości; obszar, na którym częstotliwości mogą być wykorzystywane; okres obowiązywania decyzji.

W związku z określeniem w powyżej wskazanych przepisach katalogu informacji, jakie mogą i powinny być publikowane wskazano pytającemu, iż brak jest podstawy prawnej do publikowania kodów pocztowych właściwych dla posiadaczy pozwoleń lub właściwych dla miejsca zainstalowania radiostacji.

Odnośnie natomiast sektora telekomunikacyjnego wartym odnotowania było zagadnienie dotyczące **legalności przetwarzania danych osobowych stanowiących tajemnicę telekomunikacyjną w celu dochodzenia praw przedsiębiorcy telekomunikacyjnego względem jego klienta** (tak byłego jak obecnego) przed sądem, w szczególności w zakresie dochodzenia roszczeń. Sprawa tego rodzaju podnoszona była przez jedno ze stowarzyszeń abonentów telekomunikacyjnych, które bulwersował fakt przedstawienia w sądzie bilingów osoby korzystającej z usług telekomunikacyjnych[379].

Sprawa ta była jedną z wielu, w której organ do spraw ochrony danych osobowych miałby rozstrzygnąć kwestie związane z prawidłowym (lub nie) wywiązywaniem się z umów zawieranych pomiędzy stronami w obrocie gospodarczym, ale też weryfikować prawidłowość przebiegu postępowania sądowego w odniesieniu do dowodów w sprawie prowadzonej przed sądem powszechnym[380]. W odpowiedzi Generalny inspektor zauważył, iż zgodnie z art. 233 § 1 i art. 227 ustawy Kodeks postępowania cywilnego, to sąd ocenia wiarygodność i moc dowodów według własnego przekonania, na podstawie wszechstronnego rozważenia zebranego materiału, i - przede wszystkim - to sąd decyduje o dopuszczeniu określonego dowodu biorąc przy tym pod uwagę, czy dany fakt ma istotne znaczenie dla sprawy.

Generalny Inspektor wskazał, iż prawem dostawcy usług telekomunikacyjnych jest wystąpienie z pozwem cywilnym zawierającym uzasadnienie roszczenia w postaci informacji stanowiących tajemnicę telekomunikacyjną, i zawierających dane osobowe w rozumieniu

[379] DOLiS-035-3377/14.

[380] Ocena czynności podejmowanych przez sąd w toku prowadzonego postępowania cywilnego, w tym celowości włączenia do materiału dowodowego określonych informacji, powinna być przedmiotem rozważań na gruncie ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2014 r. poz. 101 z późn zm.).

ustawy o ochronie danych osobowych. Uzasadniające takie uprawnienie przepisy prawa zawarte są w ustawie Prawo telekomunikacyjne stanowiąc, w art. 159 ust. 2 i 4 o wyjątkach od obowiązku zachowania tajemnicy telekomunikacyjnej, w tym sytuacjach, gdy przetwarzanie informacji objętych tajemnicą jest konieczne w zgodnej z prawem praktyce handlowej dla celów zapewnienia dowodów transakcji handlowej także na podstawie odrębnych przepisów.

Wykorzystanie więc danych objętych tajemnicą telekomunikacyjną abonenta w celu dochodzenia praw dostawcy usług telekomunikacyjnych przed sądem nie będzie stanowić naruszenia ww. tajemnicy[381].

Wciąż wiele wątpliwości dotyczyło praktyk **telefonicznego weryfikowania tożsamości rozmówców**, w szczególności klientów firm, przez operatorów telekomunikacyjnych[382], ale też operatorów energetycznych[383],czy firmy windykacyjne[384], w tym wykorzystywania do tego celu numeru PESEL.

W takich sprawach Generalny Inspektor wskazywał, iż wybór konkretnych procedur, czy środków, jakie należy zastosować w celu zapewnienia odpowiedniej ochrony danych osobowych nie wynika wprost z przepisów ustawy o ochronie danych osobowych ani z rozporządzeń wykonawczych do niej. Zarówno ustawa o ochronie danych osobowych, jak i rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, wskazują wprawdzie zakres minimalnych rozwiązań funkcjonalno-prawnych, jakie powinny być spełnione, ale nie na sposób, czy środki organizacyjne, przy użyciu których powinny być one osiągnięte.

Przedmiot działalności przedsiębiorców szeroko rozumianego sektora telekomunikacyjnego jest szczególnym obszarem, dla którego bezpieczeństwo i ochrona prywatności to nie tylko sprawa ochrony danych osobowych, ale także bezpieczeństwo i

---

[381] Jednocześnie, zgodnie z art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych przetwarzanie danych osobowych jest dopuszczalne, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Zgodnie z ust. 4 tego przepisu, za prawnie usprawiedliwiony cel uznaje się dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej. Ponadto zgodnie z przepisami kodeksu postępowania cywilnego, strony są obowiązane wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne. Dodatkowo zaś, art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, dopuszcza przetwarzanie danych osobowych, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Uprawnienia te czy obowiązki mogą tu wynikać z przepisów z zakresu prawa karnego czy cywilnego oraz procedury obowiązującej w tym zakresie.

[382] DOLiS-035-4267/14, DOLiS-035-4289/14, DOLiS-035-1565/14.

[383] DOLiS-035-3209/14.

[384] DOLiS-035-1565/14.

pewność obrotu gospodarczego w aspekcie zawieranych umów. W myśl natomiast art. 161 ust. 2 pkt 5 ustawy Prawo Telekomunikacyjne, a zatem z mocy prawa – dostawca publicznie dostępnych usług telekomunikacyjnych w celu wykonania umowy jest uprawniony do przetwarzania numeru ewidencyjnego PESEL. Stanowi on także dane osobowe ściśle powiązane z konkretną osobą identyfikującą ją w stosunkach publiczno-prawnych, w tym przy zawieraniu umów.

W trakcie rozmowy telefonicznej, ze względów oczywistych, konieczna jest wzajemna weryfikacja tożsamości rozmówców, numer PESEL natomiast stanowi daną osobową ściśle powiązaną z konkretną osobą identyfikującą ją w stosunkach publiczno-prawnych, w tym przy zawieraniu umów.

Zgodnie z zasadą adekwatności przetwarzania danych, wyrażoną w art. 26 ust. 1 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w tym określić takie metody weryfikacji, aby zadośćuczynić wymogom art. 36 ustawy o ochronie danych osobowych. Należy też zauważyć, iż z powodów racjonalnych np. w stosunkach przedsiębiorca telekomunikacyjny – klient, korzystnym także dla klienta jest telefoniczny sposób komunikowania się.

W celu więc weryfikacji danych klienta proponowane jest zarazem używanie innych danych, niż jego numer identyfikacyjny PESEL, np. kodu umowy, czy odrębnego identyfikatora – numeru klienta, jakkolwiek użycie do tego celu numeru PESEL nie przesądza o nielegalności przedmiotowego rozwiązania.

Jeżeli jednak telefoniczna forma kontaktu z administratorem danych w ocenie określonej osoby nie sprzyja ochronie jej danych osobowych, osoba ta może zaproponować, jako wyłączny sposób kontaktu, np. tradycyjną korespondencję listowną.

W przedmiocie działalności gospodarczej prowadzonej za pomocą Internetu, warto wskazać, iż w omawianym okresie sprawozdawczym do Biura GIODO wpłynęło około 80 zapytań dotyczących zarówno wymogów stawianych administratorom danych, którzy chcą rozpocząć działalność „w sieci", dotyczących wszelkich aspektów z tym związanych.

Między innymi pytania te dotyczyły: 1) obowiązku zgłoszenia zbiorów danych osobowych do rejestracji w ogólnokrajowym, jawnym rejestrze zbiorów prowadzonym przez Generalnego Inspektora, 2) rozwiązań organizacyjnych i technicznych dotyczących zabezpieczeń, 3) identyfikacji właściwej podstawy prawnej (np. art. 23 ust. 1 pkt 1 i 2), 4) zakresu przetwarzanych danych, 4) sposobów wypełnienia obowiązku informacyjnego, o

którym mowa w art. 24 i 25 ustawy o ochronie danych osobowych, i in. W sprawach tych Generalny Inspektor udzielał odpowiedzi, które ułatwiły rozpoczęcie, czy też prowadzenie działalności gospodarczej, jak i dochodzenie swych praw przez obywateli. Wiele z tych pytań wymagało przypomnienia podstawowych, wynikających z ustawy o ochronie danych osobowych obowiązków administratorów danych. W tym miejscu podkreślenia wymaga fakt, że w roku 2014 do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło około **50 zapytań** dotyczących spamu[385].

8.1.8. Monitoring.

Wiele pytań kierowanych do GIODO w okresie sprawozdawczym dotyczyło kwestii stosowania monitoringu wizyjnego. Jako przykład wskazać można **zapytanie od dyrekcji jednego ze szpitali, w którym planowana była instalacja takiego systemu**[386].

W odpowiedzi Generalny Inspektor wskazał, iż wprawdzie ustawa o ochronie danych osobowych nie reguluje w sposób szczególny kwestii przetwarzania danych wizualnych i dźwiękowych, ale jednak takie dane mogą być również – po spełnieniu określonych warunków – traktowane jako dane osobowe.[387] GIODO wskazał też na opinię nr 4/2004 Grupy Roboczej art. 29[388], w której zwrócono uwagę m. in. na konieczność respektowania zasady proporcjonalności (dane muszą być adekwatne i istotne dla celów przetwarzania) przy posługiwaniu się wideonadzorem, która oznacza przede wszystkim, że urządzenia monitoringu wizyjnego 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, nie wymagające 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

[385] Informacje w tym w temacie zamieszczone są na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych, pod adresem www.giodo.gov.pl., w szczególności pod adresem http://www.giodo.gov.pl/318/id_art/8304/j/pl/.

[386] DOLiS-035-1581/14.

[387] Odnosząc się do kwestii czy w przypadku stosowania monitoringu wizyjnego dochodzi do przetwarzania danych w zbiorze, należy wskazać na stanowisko doktryny, zgodnie z którym „zawartość zbioru tworzyć mogą dane (informacje) wyrażone w różny sposób – słowem, dźwiękiem (...), obrazem" (J. Barta. P. Fajgielski, R. Markiewicz, „Ochrona Danych Osobowych. Komentarz", publ. LEX Nr 106659). Pogląd ten został również wyrażony w wyrokach Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 kwietnia 2013 r. (sygn. akt II SA/Wa 211/13) oraz z dnia 9 lipca 2014 r. (sygn. akt II SA/Wa 2393/13).

[388] Powołanej na mocy art. 29 Dyrektywy nr 95/46/WE, jako niezależnego podmiotu o charakterze doradczym.

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 wizyjnego, zgodnie z wymogami art. 10 i 11 ww. Dyrektywy 95/46/WE. Wskazano przy tym, iż osoby te muszą mieć świadomość faktu prowadzenia czynności wideonadzoru, tablice informacyjne o monitoringu wizyjnym powinny być widoczne, syntetyczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Muszą także wskazywać cele działań nadzoru jak również administratora przetwarzania. Natomiast wymiary tablic muszą być proporcjonalne do miejsca, w którym są umieszczone.

Natomiast w odniesieniu do instalowania monitoringu w szpitalach, Generalny Inspektor zauważył, że przetwarzanie danych osobowych pacjentów przez zakład opieki zdrowotnej odbywa się m.in. na podstawie przepisów ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2012 r. poz. 159 z późn. zm.) oraz rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. z 2014 r. poz. 177). Rozdział 4 wyżej wymienionej ustawy reguluje prawo pacjenta do ochrony tajemnicy informacji z nim związanych, zwalniając z obowiązku jej zachowania m.in. gdy pacjent lub jego przedstawiciel ustawowy wyraża na to zgodę. Przepisy te jednak nie odnoszą się wprost do kwestii stosowania w szpitalach kamer monitoringu.

Również przepisy ogólne ustawy o ochronie danych osobowych traktują dane o stanie zdrowia jako szczególnie chronione i zapewniają im wysoki reżim ochrony[389]. Tym samym, - w obecnym stanie prawnym nie jest możliwe bezwarunkowe stosowanie monitoringu wizyjnego w szpitalach. Ewentualne zaś jego stosowanie w miejscach mających szczególne znaczenie dla wypełnienia zadań świadczenia opieki medycznej powinno łączyć się w pierwszej kolejności z rzetelnym poinformowaniem osób, których dane osobowe są przetwarzane o wszystkich istotnych okolicznościach związanych z tym procesem.

W minionym okresie sprawozdawczym zasługującym na uwagę było również zapytanie dotyczące **wykorzystywania prywatnych nagrań zdarzeń drogowych, utrwalonych na nośnikach niebędących rejestratorami** (w rozumieniu ustawy Prawo o ruchu drogowym) w

[389] Zgodnie z art. 27 ust. 1 ustawy, przetwarzanie takich danych jest co do zasady zabronione.

kontekście problemów natury prawnej dotyczących przetwarzania danych osobowych, jakie mogą się z tym zjawiskiem wiązać[390].

W odpowiedzi na pismo, jakie w tej sprawie skierowała do urzędu grupa senatorów, Generalny Inspektor na wstępie wskazał, iż dane wizualne i dźwiękowe niewątpliwie można, po spełnieniu wskazanych warunków traktować jako dane osobowe. O ile pozyskiwanie danych i dalsze ich przetwarzanie realizowane jest wyłącznie w celach prywatnych, nie jest konieczne wypełnienie obowiązków wynikających z przepisów ustawy o ochronie danych osobowych[391]. Nie oznacza to jednak, że dane osobowe utrwalone na amatorskich nagraniach zdarzeń drogowych mogą być pozyskiwane na zasadach pełnej dowolności. W każdym przypadku należy wziąć pod uwagę cel takiego działania i odpowiednio wyważyć interesy zarówno osoby, która np. mogła zostać poszkodowana podczas danego zdarzenia, jak i jego sprawcy oraz osób trzecich uwiecznionych na nagraniu.

Generalny Inspektor wskazał, iż praktyka ta budzi wątpliwości w świetle przepisów obowiązującego prawa, z uwagi na to, że po pierwsze, stanowi ingerencję w prawo do prywatności, szczególnie, że odbywa się bez wiedzy i zgody nagrywanych osób, po drugie, jest realizowana na warunkach nieznanych prawu polskiemu, niezależnie od działań służb powołanych do ścigania sprawców przestępstw, dla których to służb ustawodawca stworzył odpowiednie instrumentarium[392].

Wizerunek, jako dobro osobiste, podlega ochronie zgodnie z art. 23 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2014 r. poz. 121 z późn. zm.). Kwestia ta regulowana jest również przez przepisy ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.).

Do naruszenia dóbr osobistych może dochodzić poprzez publikowanie nagrań w Internecie. Podejmowanie takich działań w celu np. piętnowania czy wyśmiewania zachowań innych kierowców, może prowadzić także do stygmatyzacji utrwalonych na nagraniach osób -

---

[390] DOLiS-035-1868/14.

[391] Zgodnie z zgodnie z art. 3a ust. 1 ustawy o ochronie danych osobowych, ustawy nie stosuje się do: 1) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych; 2) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych. Ustawy, z wyjątkiem przepisów art. 14-19 i art. 36 ust. 1, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

[392] Możliwość wykorzystywania rejestratorów na zasadach określonych w ustawie z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2012 r. poz. 1137 z późn. zm.), zatrzymywania i legitymowania sprawców naruszeń, itp.

– zwłaszcza wobec faktu, iż nie mają one świadomości, że ich dane są pozyskiwane i w jaki sposób są dalej wykorzystywane. W rezultacie, osoba, której dane są przetwarzane w opublikowanym w sieci nagraniu, może zostać *de facto* uznana za winną naruszenia przepisów w momencie, gdy nie została jeszcze wszczęta w stosunku do niej jakakolwiek procedura. Stoi to w sprzeczności z zasadami prawa do obrony i domniemania niewinności, wyrażonymi w art. 42 Konstytucji RP. Ocena, czy amatorskie nagrania mogą być wykorzystywane dla celów dowodowych, każdorazowo powinna być dokonywana w sposób indywidualny, po wszczęciu stosownego postępowania[393].

W każdym przypadku wykorzystywania prywatnych nagrań zdarzeń drogowych, utrwalonych na nośnikach niebędących rejestratorami, oceniając konkretną sytuację i uwzględniając interesy wszystkich stron, należy wziąć pod uwagę celowość i proporcjonalność takiego działania, przepisy ustawy o ochronie danych osobowych, jak i odpowiednie przepisy szczególne.

W polskim porządku prawnym brak jest przepisów regulujących w sposób kompleksowy monitoring wizyjny. Tę lukę w przepisach ma wypełnić ustawa o monitoringu wizyjnym, do której projekt założeń przygotowało Ministerstwo Spraw Wewnętrznych. Generalny Inspektor Ochrony Danych Osobowych wielokrotnie podkreślał konieczność wprowadzenia takiej regulacji (m.in. w wystąpieniu skierowanym do Ministra Spraw Wewnętrznych i Administracji z 24 sierpnia 2011 r.[394]) i jest zarówno inspiratorem, jak i aktywnym uczestnikiem trwających obecnie prac legislacyjnych w tym zakresie[395].

8.1.9. Inne zagadnienia dotyczące ochrony danych osobowych.

W minionym okresie sprawozdawczym Generalny Inspektor odpowiedział również na **pytanie dotyczące problemu z uzyskiwaniem pisemnej zgody od osób zgłaszających przypadki niepożądane działań kosmetyków**[396].

Kwestia podstaw prawnych przetwarzania danych osobowych, w tym danych wrażliwych w związku ze zgłaszaniem i oceną przypadków niepożądanych działań

[393] Pamiętać również trzeba, że to, w jaki sposób traktowane będą takie nagrania, będzie zależało również od rodzaju pozyskującego i gromadzącego je podmiotu – zastosowanie znajdą zatem przepisy np. ustawy z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2011 r. Nr 270 poz. 1599, z późn. zm.), ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2011 r. Nr 287 poz. 1687, z późn. zm.) czy ustawy z dnia 26 stycznia 1984. – Prawo prasowe (Dz. U. z 1984 r. Nr 5, poz. 24 z późn. zm.) (w przypadku zbierania nagrań np. przez stację telewizyjną). W przypadku publikowania nagrań w Internecie pod uwagę trzeba będzie również brać przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422).

[394] GI-035-12/11

[395] DOLiS-033-523/13

[396] DOLiS-035-1672/14

kosmetyków, była już przedmiotem spotkania oraz korespondencji między Polskim Związkiem Przemysłu Kosmetycznego a Generalnym Inspektorem Ochrony Danych Osobowych w 2009 r.[397]. Po przeprowadzeniu analizy obowiązujących przepisów prawa Generalny Inspektor Ochrony Danych Osobowych wskazał na właściwe przepisy ustawy z dnia 12 grudnia 2003 r. o ogólnym bezpieczeństwie produktów (Dz. U. z 2015 r. poz. 322 z późn. zm.) oraz przepisy ustawy z dnia 30 kwietnia 2001 r. o kosmetykach (Dz. U. z 2013 r. poz. 475 z późn. zm.) ustawy o kosmetykach[398].

W wyjaśnieniach Generalny Inspektor Ochrony Danych Osobowych poinformował, że określając zasady monitorowania bezpieczeństwa kosmetyków i obowiązki podmiotów odpowiedzialnych w tym zakresie właściwe przepisy powinny również w sposób bezpośredni, jasny i adekwatny do potrzeb określać sposób realizacji takich obowiązków. Obowiązujący w chwili obecnej stan prawny w dalszym ciągu budzi pewne wątpliwości.

Nie jest możliwe potwierdzenie przez Generalnego Inspektora Ochrony Danych Osobowych, że zarządzając zgłoszeniami działań niepożądanych zarówno instytucje, lekarze, jak i przedsiębiorcy sektora kosmetycznego mogą skorzystać z art. 27 ust. 2 pkt 2 lub 3 ustawy o ochronie danych osobowych, bez pisemnej zgody konsumenta[399]. Wyjaśniono, iż zgodnie z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie ww. danych jest dopuszczalne, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. Gdyby przesłanką przetwarzania danych osobowych o stanie zdrowia miałaby być natomiast zgoda osoby, której dane dotyczą - stosownie do art. 27 ust. 2 pkt 1 ustawy – oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych - musiałoby mieć formę pisemną. Generalny Inspektor Ochrony Danych Osobowych nie ma zaś uprawnień, aby zezwolić na obejście wymaganej przepisem prawa formy. Natomiast przesłanka z art. 27 ust. 2 pkt 3 ma zastosowanie jedynie do tych przypadków, kiedy osoba, której dane dotyczą nie jest fizycznie lub prawnie zdolna do wyrażenia zgody.

---

[397] M.in. pismo PZPK z 1 lipca 2009 r. PZPK/2009/19, Pismo GIODO z dnia 13 października 2009 r. DOLiS-074-10/09/37284.

[398] Art. 2 ust. 2 i art. 10 ust. 2-6 ustawy o ogólnym bezpieczeństwie produktów, art. 11 ust. 1 pkt 5 ustawy o kosmetykach Do przepisów takich należą obecnie również przepisy Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1223/2009 z dnia 30 listopada 2009 r. dotyczącego produktów kosmetycznych. Dz. U. UE L.2009.342.59.

[399] Przetwarzanie danych szczególnie chronionych, określonych w art. 27 ust. 1 ustawy (np. dane o stanie zdrowia) może odbywać się jedynie na podstawie art. 27 ust. 2 pkt 1-10 ustawy, w przedmiotowym aspekcie można jedynie rozpatrywać przesłanki określone w art. 27 ust. 2 pkt 1-3.

Dlatego podstaw dla przetwarzania danych osobowych w związku ze zgłaszaniem przypadków niepożądanych kosmetyków należy poszukiwać przede wszystkim w przepisach szczególnych regulujących zasady i sposób wykonywania określonej działalności.

W tym kontekście należy zwrócić uwagę na nowe regulacje związane ze zgłaszaniem działań niepożądanych produktów leczniczych, które wyszły naprzeciw istotnym trudnościom podmiotów odpowiedzialnych w zakresie rejestrowania takich zgłoszeń. Przed uchwaleniem takich rozwiązań legislacyjnych Generalny Inspektor sugerował podmiotom, które zgłaszały problemy związane z brakiem wyraźnych podstaw prawnych do prowadzenia rejestrów przypadków niepożądanych produktów leczniczych przez podmioty odpowiedzialne, postulowanie przez nie wprowadzenia do porządku prawnego odpowiednich w tym zakresie regulacji. W konsekwencji ustawą z dnia 27 września 2013 r. o zmianie ustawy - Prawo farmaceutyczne oraz niektórych innych ustaw (Dz. U. z 2013 r. poz. 1245) zdefiniowano instrument „zgłoszenia pojedynczego przypadku działania niepożądanego", zaś w art. 8 tej ustawy wprowadzono do ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2012 r. poz. 159 i 742) rozdział dotyczący prawa pacjenta lub jego przedstawiciela ustawowego lub opiekuna faktycznego do zgłaszania działań niepożądanych produktów leczniczych osobom wykonującym zawód medyczny lub Prezesowi Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych lub podmiotowi odpowiedzialnemu za wprowadzenie produktu leczniczego do obrotu działania niepożądanego produktu leczniczego. Uprawnieniu pacjenta odpowiada przewidziany w art. 36g ust. 1 pkt 2 i 3 ustawy Prawo farmaceutyczne obowiązek podmiotu uprawnionego do wdrożenia i utrzymywania systemu zbierającego i zestawiającego w jednym rejestrze zgłoszeń pojedynczych przypadków działań niepożądanych, które są kierowane do tego podmiotu. W art. 36e tej ustawy dokładnie określono zakres danych, które rejestrowane są w związku ze zgłoszeniem.

Powyższe regulacje niewątpliwie w sposób precyzyjny przewidują uprawnienie do prowadzenia rejestrów przypadków działań niepożądanych produktów leczniczych. Być może mogłyby one być dla podstawą dla Polskiego Związku Przemysłu Kosmetycznego i Głównego Inspektoratu Sanitarnego do przeprowadzenia odpowiednich analiz pod kątem sformułowania postulatów *de lege ferenda* i skierowania ich do właściwego resortu wyposażonego w inicjatywę legislacyjną z uwzględnieniem istniejących w tym zakresie potrzeb i dotychczasowych doświadczeń podmiotów zainteresowanych. Odpowiednie zmiany w obowiązującym stanie prawnym niewątpliwie mogą wyeliminować zgłaszane wątpliwości.

Do GIODO zwrócono się z pytaniem, **czy przewoźnik wykonujący transport węgla kamiennego stanowiącego deputat węglowy wypłacany emerytom górnikom w naturze ma prawo żądać od emeryta górnika wypisania na okazanym druku wszystkich swoich danych osobowych włącznie z numerem PESEL**[400].

W odpowiedzi GIODO wyjaśnił, że aby móc prawidłowo realizować wymienione uprawnienie potrzebna jest jednoznaczna identyfikacja uprawnionej osoby. Przewoźnik musi bowiem dostarczyć deputat konkretnej uprawnionej osobie. Identyfikacja taka wymaga najczęściej podania podstawowego zestawu danych osobowych, do którego obok imienia i nazwiska oraz adresu, należy również numer PESEL[401].

Abstrahując od uprawnień do deputatu węglowego warto podnieść, że w każdej sytuacji, gdy pojawiają się wątpliwości dotyczące podstaw prawnych czy celu pozyskiwania - lub dysponowania danymi osobowymi w tym numeru PESEL określonej osoby, osoba ta ma prawo zwrócić się do podmiotu żądającego podania takich danych z wnioskiem o informacje na ten temat[402].

Generalny Inspektor Ochrony danych Osobowych otrzymał również zapytanie, **czy instytucja kulturalna może zażądać okazania dowodu osobistego przy wejściu na spektakl**[403]. Konieczność weryfikacji tożsamości miała miejsce w przypadku tzw. biletów elektronicznych (zakupionych za pośrednictwem Internetu), na których nadrukowane było imię i nazwisko osoby kupującej.

W odpowiedzi wskazano przede wszystkim, iż uprawnienie do legitymowania osób w celu ustalenia ich tożsamości przysługuje wyłącznie tym podmiotom, którym zostało ono zagwarantowane w obowiązujących przepisach prawa[404]. Podmioty, którym takie uprawnienie nie zostało przyznane wprost w przepisach prawa, mogą przetwarzać dane osobowe, jednakże bez prawa do żądania od osób wchodzących na teren określonego obiektu

---

[400] DOLiS-035-2044/14.

[401] Ustawa z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2010 r., poz. 388 z późn. zm.) w art. 15-ust. 2 wskazuje, iż numer PESEL jest 11-cyfrowym, stałym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną.

[402] Uprawnienia te zostały określone w przepisach art. 24 ust 1 pkt 4 i art. 32-35 ustawy o ochronie danych osobowych.

[403] DOLiS-035-314/14.

[404] Zaliczyć do nich należy m.in. Policję (art. 15 ust. 1 pkt 1 ustawy z dnia 6 kwietnia 1990 r. o Policji – Dz. U. z 2011 r. Nr 287 poz. 1687 z późn. zm.), Straż Graniczną (art. 11 ust. 1 pkt 4 ustawy z dnia 12 października 1990 r. o Straży Granicznej – Dz. U. z 2011 r. Nr 116 poz. 675 z późn. zm.), Służbę Więzienną (art. 18 ust. 1 pkt 1 ustawy z dnia 26 kwietnia 1996 r. o Służbie Więziennej – Dz. U. z 2014 r. poz. 173 z późn. zm.), Centralne Biuro Antykorupcyjne (art. 14 ust. 1 pkt 2 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym – Dz. U. z 2012 r. poz. 621 z późn. zm.), czy pracowników ochrony w rozumieniu przepisów ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2005 r. Nr 145 poz. 1221 z późn. zm.) – art. 36 ust. 1 pkt 1.

okazania dokumentu tożsamości, celem ustalenia ich tożsamości lub potwierdzenia podanych przez nich danych osobowych w dokumencie tym zawartych. Przetwarzanie danych osobowych przez te podmioty jest możliwe na zasadach ogólnych – stosownie do przepisów ustawy o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne w momencie spełnienia jednej z przesłanek wymienionych w art. 23 ust. 1 pkt 1-5 ustawy.

Jednocześnie, aby można było mówić o zgodności procesu przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych, ich administrator musi dopełnić szeregu innych obowiązków, m.in. dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane[405]. Administrator danych może zatem przetwarzać, w tym pozyskiwać jedynie takie dane, które są niezbędne do osiągnięcia zamierzonego celu.

Nie wydaje się, by ustalenie tożsamości było działaniem niezbędnym do umożliwienia wejścia na spektakl, a zatem powstała wątpliwość, czy w niniejszej sprawie został spełniony wymóg adekwatności – zwłaszcza, że zgodnie z przedstawionym w korespondencji stanem faktycznym, w przypadku tradycyjnych biletów zakupionych w kasie dane osobowe nie były pozyskiwane i nie była konieczna ich późniejsza weryfikacja.

8.1.10. 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).

[405] Wymóg wynikający z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

W 2014 roku Generalny Inspektor Ochrony Danych Osobowych skierował **66 takich wystąpień.**

Poniżej przedstawione zostały przykłady wystąpień Generalnego Inspektora skierowanych do **podmiotów administracji publicznej i podmiotów prywatnych**.

Pismem z dnia 10 marca 2014 r.[406] na podstawie art. 19a ust. 1 ustawy ochronie danych osobowych Generalny Inspektor skierował do jednego ze starostw powiatowych wystąpienie **w związku z upublicznianiem na stronie internetowej urzędu (umożliwiającej przeglądanie map należących do starostwa powiatowego) m.in. numerów ksiąg wieczystych poszczególnych nieruchomości**. Generalny Inspektor wskazał, iż takie upublicznienie nie jest zgodne z przepisami prawa.

Generalny Inspektor w ww. wystąpieniu, a następnie w kolejnym piśmie z dnia 1 sierpnia 2014 r. podniósł, w odniesieniu do umieszczenia na ogólnie dostępnej stronie internetowej starostwa numerów ksiąg wieczystych poszczególnych nieruchomości, że dane zawarte w ewidencji gruntów i budynków oraz w operacie ewidencyjnym mogą mieć charakter przedmiotowy, podmiotowy, bądź podmiotowo-przedmiotowy. W ocenie Generalnego Inspektora powszechnie dostępne dla wszystkich podmiotów mogą być jedynie informacje, które mają charakter przedmiotowy, tj. odnoszą się gruntów, budynków, a nie do ich właścicieli (podobne tezy znajdują oparcie w orzecznictwie sądowo-administracyjnym[407]).

---

[406] DOLiS-035-138/14.

[407] Stosownie do wyroku Wojewódzkiego Sądu Administracyjnego we Wrocławiu z dnia 2 grudnia 2010 r (sygn. II SA/Wr 546/2010) „Udzielanie na żądanie wszystkich zainteresowanych w trybie art. 24 ust. 2 p.g.k. informacji o gruntach, budynkach i lokalach mogą być tylko informacje o charakterze przedmiotowym, a więc nie zawierające danych podmiotowych, o których mowa m.in. w art. 20 ust. 2 pkt 1 p.g.k.". W uzasadnieniu wyroku Sąd zwrócił ponadto uwagę, iż: „ukształtował się powszechnie przyjęty w orzecznictwie sądów administracyjnych pogląd, że przedmiotem ewidencji gruntów i budynków są dane o charakterze przedmiotowym (art. 20 ust. 1 i ust. 2 pkt 3 i 4 p.g.k.) oraz dane o charakterze podmiotowym (art. 20 ust. 2 pkt 1 i pkt 2 p.g.k.) (por. np. wyrok NSA z dnia 20 listopada 2009 r. I OSK 189/2009, wyrok NSA z dnia 21 lipca 2010 r. I OSK 1312/2009; wyrok NSA z dnia 19 maja 2010 r. I OSK 1030/2009, wyrok WSA w Gliwicach z 28 października 2010 r. II SA/Gl 668/2010 www.orzeczenia.nsa.gov.pl). Przy czym podkreślić należy, że udzielanie na żądanie wszystkich zainteresowanych w trybie art. 24 ust. 2 p.g.k. informacji o gruntach, budynkach i lokalach mogą być tylko informacje o charakterze przedmiotowym, a więc nie zawierające danych podmiotowych, o których mowa m.in. w art. 20 ust. 2 pkt 1 p.g.k. (...) żądanie podania informacji o numerach ksiąg wieczystych nieruchomości (...) dotyczy danych o charakterze podmiotowo-przedmiotowy, czyli w istocie danych osobowych. Zasadne jest tym samym stanowisko orzekających w sprawie organów, że wnioskodawca winien był w tej sytuacji - zgodnie z art. 24 ust. 5 pkt 3 p.g.k. - wykazać interes prawny w uzyskaniu informacji podmiotowo-przedmiotowej." Powyższe stanowisko potwierdza również wyrok z 4 lutego 2014 r. Wojewódzkiego Sądu Administracyjnego w Lublinie (sygn. akt III SA/Lu 638/13), zgodnie z którym „Organy prawidłowo odwołały się do art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), zgodnie z którym za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. (...) Za dane osobowe w rozumieniu ustawy należy uznać numery ksiąg wieczystych i zbiorów dokumentów, skoro w tych księgach i zbiorach są ujawnione podmioty będące właścicielami nieruchomości, dla których księgi te lub zbiory są prowadzone. Skoro treść ksiąg wieczystych i zbiorów dokumentów jest powszechnie dostępna (księgi wieczyste w sądach i

Numer księgi wieczystej jest informacją o charakterze podmiotowo-przedmiotowym, która jednocześnie wypełnia ustawową definicję danej osobowej i podlega ochronie przewidzianej w ustawie o ochronie danych osobowych. Danymi osobowymi są zarówno informacje o numerach ksiąg wieczystych prowadzonych dla nieruchomości stanowiących własność osób fizycznych, jak i wszelkie dane zawarte w treści ksiąg wieczystych dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych.

Warunkiem uzyskania dostępu do odpisu księgi wieczystej (zwykłego, bądź zupełnego, a więc zawierającego dane osobowe także byłych właścicieli nieruchomości, dla której księga była prowadzona) jest konieczność podania jej numeru. Wobec jawności ksiąg wieczystych oraz wprowadzenia przez Ministerstwo Sprawiedliwości projektu informatycznego tzw. Nowa Księga Wieczysta, umożliwiającego m.in. bezpośredni wgląd do ksiąg wieczystych w systemie informatycznym, po uprzednim podaniu numeru księgi wieczystej, bez trudu można uzyskać dostęp do zawartych w niej informacji. Udostępnianie przez starostę na ogólnodostępnej stronie internetowej numerów ksiąg wieczystych naniesionych na mapy będące w posiadaniu starostwa prowadzi do sytuacji, w której osoby zapoznające się z treścią udostępnionego dokumentu mogą w sposób niewymagający nadmiernych kosztów, czasu lub działań zapoznać się zawartymi w księdze danymi osobowymi osób będących, np. właścicielami nieruchomości, dla której prowadzona jest dana księga wieczysta.

W zakresie dostępu do ksiąg wieczystych obowiązuje zasada jawności ksiąg wieczystych, która ma fundamentalne znaczenie dla obrotu prawnego nieruchomościami. Pamiętać jednak należy, że jawność materialna i formalna ksiąg wieczystych nie oznacza dowolnego dostępu do tych ksiąg. Zasady i formy dostępu do ksiąg wieczystych zostały przez ustawodawcę starannie unormowane. Dostęp do ksiąg wieczystych nie jest zatem dowolny, a do przeglądania treści księgi wieczystej, w tym za pomocą sytemu teleinformatycznego niezbędnym warunkiem jest znajomość dokładnego numeru księgi wieczystej. Bez dokładnej znajomości powyższego numeru nie można zapoznać się z treścią księgi wieczystej.

---

większość w Internecie poprzez portal dostępowy, zbiory dokumentów w sądach) to ujawnienie ich numerów pozwala jednocześnie na ujawnienie danych osobowych wpisanych w tych księgach właścicieli nieruchomości oraz danych osobowych właścicieli nieruchomości ujawnionych w dokumentach złożonych do zbiorów dokumentów. Można zatem stwierdzić, że dane z ewidencji gruntów i budynków dotyczące numerów ksiąg wieczystych i zbiorów dokumentów zawierają dane osobowe podmiotów, o których mowa w art. 20 ust. 2 pkt 1 p.g.i k. Organ ewidencyjny prawidłowo uzależnił udzielenie skarżącej Spółce żądanych informacji od wykazania interesu prawnego. Wnioskodawca żądając podania numeru księgi wieczystej lub zbioru dokumentów dla nieruchomości nie wykazał interesu prawnego, a więc zasadnym było wydanie decyzji odmawiającej udzielenia żądanej informacji."

Znajomość numeru księgi stanowi zatem barierę przed niepożądanym dostępem do treści księgi wieczystej np. przed pozyskaniem danych osobowych z księgi wieczystej w celach marketingowych. W tym zakresie znajomość numeru księgi wieczystej z jednej strony ogranicza niebezpieczeństwo pozyskiwania z księgi danych osobowych w celach innych niż wynika to z ustawy o księgach wieczystych i hipotece. Z drugiej strony urzeczywistnia ochronę danych osobowych wynikającą z przepisów ustawy o ochronie danych osobowych.

Potwierdzeniem powyższego rozumowania jest fakt, że zgodnie z przepisami ustawy z dnia 24 maja 2013 r. o zmianie ustawy o księgach wieczystych i hipotece (Dz. U. poz. 941) do systemu ksiąg wieczystych wprowadzony został nowy instrument prawny w postaci wyszukiwania ksiąg wieczystych w centralnej bazie danych ksiąg wieczystych, za pomocą zdefiniowanego kryterium wyszukania (np. danych identyfikacyjnych nieruchomości, danych osobowych właściciela). Wyszukiwanie ksiąg wieczystych w CBDKW (Centralna Baza Dokumentów Ksiąg Wieczystych) jest nową instytucją mającą gwarantować sprawne i skuteczne realizowanie uprawnień przysługujących państwu, a skonkretyzowanych w normach szczególnych, np. w celu odszukania składników majątku dłużnika w sądowym postępowaniu egzekucyjnym. Podkreślić jednak należy, że dostęp do ww. instrumentu prawnego przysługuje tylko ściśle określonym podmiotom oraz organom państwowym.

Mając powyższe na uwadze Generalny Inspektor stwierdził, że udostępnianie numerów ksiąg wieczystych na stronie internetowej starostwa prowadzi do „obejścia" przepisów ustawy o księgach wieczystych i hipotece. Skoro bowiem ustawodawca ściśle reglamentuje dostęp do numerów ksiąg wieczystych za pomocą ww. instrumentu prawnego, to uznaje tym samym, że powszechny dostęp do tego typu informacji jest niedopuszczalny. Innymi słowy, gdyby wolą ustawodawcy było wprowadzenie instrumentu prawnego umożliwiającego każdemu zainteresowanemu zapoznanie się z numerem księgi wieczystej za pomocą zdefiniowanego kryterium wyszukania (np. imienia i nazwiska właściciela, numeru jego PESEL, adresu), to wówczas nie wprowadzałby tak szczegółowych regulacji normujących przeszukiwanie ksiąg wieczystych w centralnej bazie danych ksiąg wieczystych.

Generalny Inspektor Ochrony Danych Osobowych nie podzielił reprezentowanego przez starostę stanowiska, że powszechne udostępnianie za pomocą środków komunikacji elektronicznej danych objętych ewidencją gruntów i budynków znajduje swoje prawne uzasadnienie w art. 24 ust. 2 i ust. 3 ustawy z dnia 17 maja 1989 r. Prawo geodezyjne i

kartograficzne (Dz. U. z 2010 r. Nr 193 poz. 1287 z późn. zm.)[408] w związku z art. 9 ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz. U. z 2010 r. Nr 76 poz. 489 z późn. zm.)[409]. W ocenie GIODO przyjęcie takiego stanowiska jest sprzeczne z normą zawartą w art. 24 ust. 5 ustawy Prawo geodezyjne i kartograficzne[410] i oznaczałoby, że udostępnianie tych danych nie podlega zasadom określonym w tym przepisie. Obecnie obowiązujące przepisy prawa nie przewidują upoważnienia starosty do upowszechnienia poprzez strony internetowe ewidencji gruntów i budynków w zakresie danych osobowych, o których mowa w art. 24 ust. 5 ustawy Prawo geodezyjne i kartograficzne, wobec tego działanie takie jest niezgodne z obowiązującym prawem i narusza prawo do ochrony danych osobowych obywateli[411]. Oparcie każdej formy przetwarzania danych osobowych obywateli na przepisie prawa dotyczy w szczególności podmiotów publicznych, albowiem organy

---

[408] Zgodnie z tymi przepisami, starosta udostępnia informacje zawarte w operacie ewidencyjnym w formie: 1) wypisów z rejestrów, kartotek i wykazów tego operatu; 2) wyrysów z mapy ewidencyjnej; 3) kopii dokumentów uzasadniających wpisy do bazy danych operatu ewidencyjnego; 4) plików komputerowych sformatowanych zgodnie z obowiązującym standardem wymiany danych ewidencyjnych; 5) usług, o których mowa w art. 9 ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej.

[409] Zgodnie z art. 9 ust. 1 ustawy o infrastrukturze informacji przestrzennej, organy administracji prowadzące rejestry publiczne, które zawierają zbiory związane z wymienionymi w załączniku do ustawy tematami danych przestrzennych, tworzą i obsługują, w zakresie swojej właściwości, sieć usług dotyczących zbiorów i usług danych przestrzennych, do których zalicza się usługi: 1) wyszukiwania, umożliwiające wyszukiwanie zbiorów oraz usług danych przestrzennych na podstawie zawartości odpowiadających im metadanych oraz umożliwiające wyświetlanie zawartości metadanych; 2) przeglądania, umożliwiające co najmniej: wyświetlanie, nawigowanie, powiększanie i pomniejszanie, przesuwanie lub nakładanie na siebie zobrazowanych zbiorów oraz wyświetlanie objaśnień symboli kartograficznych i zawartości metadanych; 3) pobierania, umożliwiające pobieranie kopii zbiorów lub ich części oraz, gdy jest to wykonalne, bezpośredni dostęp do tych zbiorów; 4) przekształcania, umożliwiające przekształcenie zbiorów w celu osiągnięcia interoperacyjności zbiorów i usług danych przestrzennych; 5) umożliwiające uruchamianie usług danych przestrzennych. Ust. 2. Usługi, o których mowa w ust. 1, są powszechnie dostępne za pomocą środków komunikacji elektronicznej. Ust. 3. Usługi, o których mowa w ust. 1 pkt 1, umożliwiają wyszukiwanie zbiorów i usług danych przestrzennych co najmniej według następujących kryteriów lub ich kombinacji: 1) słowa kluczowe; 2) klasyfikacja danych przestrzennych oraz usług danych przestrzennych; 3) jakość i ważność zbiorów; 4) stopień zgodności ze standardami technicznymi dotyczącymi interoperacyjności zbiorów i usług danych przestrzennych; 5) położenie geograficzne; 6) warunki dostępu i korzystania ze zbiorów oraz usług danych przestrzennych; 7) organy administracji odpowiedzialne za tworzenie, aktualizację i udostępnianie zbiorów oraz usług danych przestrzennych.

[410] Zgodnie z tym przepisem, starosta udostępnia dane ewidencji gruntów i budynków zawierające dane podmiotów, o których mowa w art. 20 ust. 2 pkt 1, oraz wydaje wypisy z operatu ewidencyjnego, zawierające takie dane, na żądanie: 1) właścicieli oraz osób i jednostek organizacyjnych władających gruntami, budynkami lub lokalami, których dotyczy udostępniany zbiór danych lub wypis; 2) organów administracji publicznej albo podmiotów niebędących organami administracji publicznej, realizujących, na skutek powierzenia lub zlecenia przez organ administracji publicznej, zadania publiczne związane z gruntami, budynkami lub lokalami, których dotyczy udostępniany zbiór danych lub wypis; 3) innych podmiotów niż wymienione w pkt 1 i 2, które mają interes prawny w tym zakresie.

[411] Warto przypomnieć, że Konstytucja RP w art. 47 statuuje prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Zgodnie z art. 51 ust. 1 i 5 Konstytucji RP nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a zasady i tryb gromadzenia oraz udostępniania informacji dotyczących osoby powinna określać ustawa. Ograniczenia w zakresie korzystania z prawa do ochrony życia prywatnego i decydowania o swoim życiu osobistym wymagają bezwzględnie regulacji rangi ustawowej (art. 31 ust. 3 Konstytucji RP).

publiczne obowiązane są do działania jedynie na podstawie i w granicach prawa[412]. Granice działań podmiotów publicznych wyznaczają wyłącznie normy prawne określające ich kompetencje, zadania i tryb postępowania.

Mając na uwadze powyższe, w świetle konstytucyjnej zasady legalizmu GIODO wezwał starostę do niezwłocznego podjęcia działań mających na celu usunięcie numerów ksiąg wieczystych z ogólnie dostępnych stron internetowych starostwa.

Pismem z dnia 2 września 2014 r. (sygn.: SP.142.1.2014) starosta poinformował, że dostęp do numerów ksiąg wieczystych na stronie internetowej starostwa będzie wyłączony do czasu do czasu ostatecznego wyjaśnienia kwestii związanych z realizacją przez starostę obowiązków określonych w ustawie z 17 maja 1989 r. Prawo geodezyjne i kartograficzne, ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, oraz w ustawie z dnia 4 marca 2010 o infrastrukturze informacji przestrzennej.

Pismem dnia 5 sierpnia 2014 r.[413] GIODO zwrócił się do Ministra Sprawiedliwości o niezwłoczne podjęcie prac legislacyjnych mających **na celu rzetelne i szczegółowe unormowanie kwestii ujawniania danych osobowych na wokandach sądowych w zależności od jawności rozprawy lub rodzaju sprawy.** Wskazał, że niewątpliwie **regulacja taka powinna znaleźć się w akcie rangi ustawowej**. GIODO podkreślił, że zamieszczanie danych osobowych na wokandach sądowych wynika obecnie z przepisów o charakterze wewnętrznym, a nie powszechnie obowiązujących, w tym Konstytucji RP.[414] Oparcie każdej formy przetwarzania, w tym udostępniania danych osobowych obywateli na przepisie prawa dotyczy w szczególności podmiotów publicznych, albowiem organy publiczne obowiązane są do działania jedynie na podstawie i w granicach prawa,[415] bowiem granice działań podmiotów publicznych wyznaczają wyłącznie normy prawne określające ich kompetencje, zadania i tryb postępowania.

W swoim wystąpieniu organ do spraw osobowych wskazał, że niewątpliwie obecna regulacja § 23 zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej (Dz. Urz. MS nr 5 poz. 22 z późn. zm.) nie spełnia powyższych kryteriów. Ponieważ regulacja ta przewiduje sporządzanie wokand w każdej sprawie niezależnie od utajnienia jej

[412] Art. 7 Konstytucji RP oraz art. 6 Kodeksu postępowania administracyjnego.
[413] DOLiS-035-278/14.
[414] Stosowne przepisy Konstytucji RP w tym zakresie przytoczono w przypisie nr 6.
[415] Art. 7 Konstytucji RP oraz art. 6 Kodeksu postępowania administracyjnego.

przebiegu, w tym umieszczanie na wokandzie danych osobowych świadków – osób poszkodowanych przestępstwem, to dochodzi do istotnej i nieproporcjonalnej ingerencji w prawo do prywatności i związane z nim prawo do ochrony danych osobowych.

Pismem z dnia 27 sierpnia 2014 r. Ministerstwo Sprawiedliwości poinformowało, że „działania legislacyjne zostały podjęte i są finalizowane. Zmiany stanu prawnego (wejścia w życie nowej regulacji) spodziewać się można w połowie 2015 r." Niemniej jednak, w ocenie Ministerstwa Sprawiedliwości zagadnienie wokandy sądowej nie wymaga regulacji ustawowej[416].

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych zajął stanowcze stanowisko[417], że **kwestia treści wokandy i sposobu jej udostępniania stanowi materię ustawową w kontekście norm konstytucyjnych oraz przepisów ustawy o ochronie danych osobowych.** Wokanda sądowa jest formą ujawniania danych osobowych, Konstytucja Rzeczypospolitej Polskiej stanowi zaś, że „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a zasady i tryb gromadzenia oraz udostępniania informacji dotyczących osoby powinna określać ustawa"[418].

Generalny Inspektor wskazał, że skoro resort sprawiedliwości podjął wysiłek w kierunku koniecznych zmian prawnych w zakresie unormowania wokand sądowych, powinno to nastąpić w akcie odpowiedniej rangi. Mocą rozporządzenia mogą być natomiast jedynie konkretyzowane regulacje ustawowe. Jest to podstawowy warunek, jaki musi być spełniony, aby nowe przepisy mogły zostać uznane za zgodne z wymogami konstytucyjnymi i nie było podstaw do kwestionowania tych przepisów przed Trybunałem Konstytucyjnym[419].

W ww. korespondencji kierowanej do Ministra Sprawiedliwości w tej sprawie, Generalny Inspektor zaoponował przeciwko rozstrzyganiu o ograniczaniu konstytucyjnej zasady jawności postępowania sądowego oraz udostępnianiu danych osobowych stron postępowania, a zatem w kwestii prawa do ochrony prywatności osób biorących udział w postępowaniu w akcie wykonawczym. Generalny Inspektor zauważył, że art. 42 § 2 i 3

---

[416] Pismo MS o sygn.: DSO-III-070-45/14.
[417] Pismo GIODO z dnia 23 października 2014 r. o sygn.: DOLiS-035-278/14/MM/83278.
[418] Art. 51 ust. 1 i 5 Konstytucji RP.
[419] Zgodnie ze stanowiskiem Trybunału Konstytucyjnego, z uzasadnienia postanowienia z dnia 31 stycznia 2007 roku (sygn. akt S 1/2007): „Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować" funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. Także art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki."

ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133) wyraźnie zastrzega, że sądy rozpoznają i rozstrzygają sprawy w postępowaniu jawnym, a rozpoznanie sprawy w postępowaniu niejawnym lub wyłączenie jawności postępowania jest dopuszczalne jedynie na podstawie przepisów ustaw[420].

Generalny Inspektor wskazał, że w polskim porządku prawnym w chwili obecnej brak jest przepisu ustawy, który upoważniałby Ministra Sprawiedliwości, do wydania rozporządzenia w tym przedmiocie, odwołując się do art. 92 Konstytucji RP. Przepis ten wyraźnie zastrzega, że rozporządzenia mogą być wydawane jedynie na podstawie szczegółowego upoważnienia zawartego w ustawie i w celu jej wykonania. Upoważnienie powinno określać organ właściwy do wydania rozporządzenia i zakres spraw przekazanych - do uregulowania oraz wytyczne dotyczące treści aktu. Jawność wokandy jest pochodną wynikającej z prawa do rzetelnego procesu zasady jawności postępowania sądowego. Sporządzanie i publikowanie wokand sądowych jest zatem przejawem jawności zewnętrznej postępowania, rozumianej jako dostępności informacji na temat przebiegu postępowania dla osób niebiorących w nim udziału. Konkretyzacja konstytucyjnej normy zawartej w art. 45 ust. 2 Konstytucji RP poprzez wskazanie jaki podmiot, w jakich sytuacjach i w jaki sposób może ograniczyć konstytucyjną zasadę jawności postępowania sądowego nie należy do władzy wykonawczej i nie może następować w drodze rozporządzenia[421].

Niestety, zarówno przepisy ustaw, uprawniając sąd do wyłączenia w całości lub w części jawności rozprawy, jak i żaden inny przepis prawa, nie dają sądowi możliwości ograniczenia treści wokandy. Podkreślenia wymaga, że wszystkie powołane przepisy są

[420] Zasadę tą umacniają i rozwijają również odpowiednie ustawowe przepisy procedury karnej i cywilnej. W odniesieniu do spraw karnych kwestię jawności i ograniczeń jawności rozprawy reguluje art. 355 (wskazujący na jawność rozprawy – co oznacza jej dostępność dla wszystkich zainteresowanych osób, poza tymi które biorą udział w postępowaniu) i następne przepisy ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89 poz. 555 ze zm.). Tytułem przykładu - art. 360 § 1 K.p.k. wskazuje w jakich przypadkach sąd wyłącza jawność rozprawy w całości albo w części. Dla spraw cywilnych (w postępowaniu procesowym) kluczowe znaczenie ma przepis art. 148 § 1 ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 2014 r. poz. 101 ze zm.) stanowiący, że jeżeli przepis szczególny nie stanowi inaczej, posiedzenia sądowe są jawne, a sąd orzekający rozpoznaje sprawy na rozprawie. Zgodnie natomiast z art. 153 § 1 K.p.c., sąd z urzędu zarządza odbycie całego posiedzenia lub jego części przy drzwiach zamkniętych, jeżeli publiczne rozpoznanie sprawy zagraża porządkowi publicznemu lub moralności lub jeżeli mogą być ujawnione okoliczności objęte ochroną informacji niejawnych. § 3 tego artykułu daje sądowi uprawnienie do zarządzenia odbycia posiedzenia lub jego części przy drzwiach zamkniętych na wniosek strony, jeżeli podane przez nią przyczyny uzna za uzasadnione lub jeżeli roztrząsane być mają szczegóły życia rodzinnego. Postępowanie dotyczące tego wniosku odbywa się przy drzwiach zamkniętych. Postanowienie w tym przedmiocie sąd ogłasza publicznie.

[421] Zgodnie z art. 45 ust. 2 Konstytucji RP, wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie.

przepisami ustawowymi i niezaprzeczalnie taką samą rangę powinny mieć przepisy uprawniające do wskazania ograniczeń treści wokandy.

Generalny Inspektor zauważył także, iż art. 31 Konstytucji RP statuuje tzw. zasadę proporcjonalności. Godząc się na limitowanie konstytucyjnych praw i wolności, ustawodawca precyzuje warunki dopuszczalności tego rodzaju ograniczeń[422].

Generalny Inspektor nie podzielił stanowiska podniesionego w ww. piśmie MS, że „w kwestii ograniczenia wokand sądowych co do zasady pierwszeństwo ma art. 45 Konstytucji RP i wyrażona w nim zasada jawności rozpoznawania spraw sądowych", i że „skoro zasada konstytucyjna wyrażona w art. 45 opatrzona jest wyraźnie od niej zaznaczonymi wyjątkami to wydaje się, że z tej normy dopuszczającej wyłączenie jawności (czyli art. 45 ust. 2 Konstytucji RP), a nie z innych norm Konstytucji wynika możliwość ograniczenia jawności i w tym zakresie może mieścić się jej ograniczenie" oraz że „norma art. 45 ust. 2 jest normą konkretyzującą ograniczenie, w odróżnieniu od ogólnej normy art. 31 ust. 3".

W ocenie Generalnego Inspektora powołane normy art. 45 ust 2 i art. 31 ust. 3 nie pozostają w kolizji, którą należałoby rozstrzygać wg reguły *lex specialis derogat legi generali*, a ramy dopuszczalnych ograniczeń wyznacza wyrażona w art. 31 ust. 3 Konstytucji zasada proporcjonalności[423].

Z powyższych względów sprawa treści i sposobu regulacji wokand sądowych jest od dłuższego czasu przedmiotem istotnych kontrowersji wyrażanych w opinii publicznej, jak i - jak wynika z przekazanych Generalnemu Inspektorowi informacji – wystąpień kierowanych do resortu sprawiedliwości przez Rzecznika Praw Obywatelskich[424] i Rzecznika Praw Dziecka[425]. W ostatnim czasie szczególne zaniepokojenie budzą przypadki ujawniania danych

---

[422] Trybunał Konstytucyjny w swym orzecznictwie wielokrotnie wskazywał, że art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej precyzyjnie określa przesłanki dopuszczalności ograniczeń w korzystaniu z wolności i praw jednostki. Należą do nich: a) ustawowa forma ograniczeń, b) funkcjonalny związek ograniczenia z realizacją wartości wskazanych enumeratywnie w art. 31 ust. 3 Konstytucji, c) istnienie konieczności ograniczeń, przy braku innych środków skutecznie służących temu celowi, d) zakaz naruszania istoty danej wolności lub prawa (wyrok TK z dnia 15 grudnia 2004 r. K. 2/2004 OTK ZU 2004/11A poz. 117; por. też np. wyrok TK z dnia 29 czerwca 2001 r. K. 23/2000 OTK ZU 2001/5 poz. 124, wyrok z dnia 12 stycznia 2000 r. P. 11/98 OTK ZU 2000/1 poz. 3).

[423] W orzecznictwie Trybunału Konstytucyjnego wskazuje się, *że* zarówno prawo do sądu, jak ochrona prawa - do prywatności i do decydowania o sobie samym nie ma charakteru absolutnego i może podlegać ograniczeniom, jeżeli przemawia za tym inna norma, zasada lub wartość konstytucyjna, a stopień tego ograniczenia pozostaje w odpowiedniej proporcji do rangi interesu, któremu ograniczenie ma służyć (zob. orzeczenie TK z dnia 24 czerwca 1997 r. K. 21/96 OTK ZU 1997/2 poz. 23; wyroki TK z dnia 21 stycznia 2014 r. SK 5/2012, a także z dnia 9 lipca 2009 r. SK 48/2005 oraz z dnia 11 października 2011 r. K. 16/2010).

[424] Informacja zawarta w skierowanym do GIODO piśmie RPO z dnia 10 marca 2015 r. o sygn.: VII.501.337.2014.KM.

[425] Informacja zawarta w skierowanym do wiadomości GIODO piśmie RPD z dnia 18 marca 2014 r. o sygn.: ZSR/500/4/2014/MM.

osobowych świadków - potencjalnych pokrzywdzonych w sprawie oskarżonego o czyny pedofilskie, w sytuacji, gdy przebieg rozprawy był utajniony, czy też ujawniania w treści wokandy przedmiotu sprawy wraz z danymi osobowymi dzieci w sprawach rodzinnych (np. w sprawach o przysposobienie). Podkreśla się, że obecny stan rzeczy jest niezgodny nie tylko z aktami prawa krajowego, ale i regulacjami aktów międzynarodowego, m.in. Konwencją o prawach dziecka (Dz. U. z 1991 r. Nr 120 poz. 526 z późn. zm.).

Pismem z dnia 30 stycznia 2015 r. Generalny Inspektor poinformował również Rzecznika Praw Obywatelskich o swoim stanowisku oraz korespondencji prowadzonej z resortem sprawiedliwości w kwestii właściwego uregulowania sprawy wokand sądowych. Wskazał, że Ministerstwo Sprawiedliwości prowadzi prace nad rozwiązaniami legislacyjnymi dotyczącymi ujawniania danych osobowych na wokandach sądowych. W resorcie trwają prace nad nowym rozporządzeniem **Regulamin urzędowania sądów powszechnych**, w którym planuje się określić zasady i sposób zamieszczania danych na wokandach sądowych.[426] Natomiast żadnych unormowań w zakresie wokand sądowych nie przewidywały procedowane w Sejmie i Senacie projekty: **rządowy projekt ustawy o zmianie ustawy - Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw** (druk sejmowy nr 2680) oraz **senacki projekt ustawy - Prawo ustroju sądów powszechnych** (druk nr 2544).[427]

W przekonaniu Generalnego Inspektora projektowane obecnie rozwiązania legislacyjne w zakresie wokand sądowych dotyczą w istocie wolności i praw człowieka i obywatela określonych w Konstytucji RP oraz w innych aktach normatywnych (ustawie o ochronie danych osobowych, Kodeksie postępowania cywilnego, Kodeksie postępowania karnego i ustawy Prawo o ustroju sądów powszechnych).

Rzecznik Praw Obywatelskich odpowiadając ww. pismem z dnia 10 marca 2015 r. na ww. pismo, podzielił wątpliwości GIODO.

---

[426] Przepisy projektu znajdujące się w rozdziale 4 „Wokandy sądowe" (§71-74). Generalny Inspektor, pismem z dnia 12 maja 2015 r. o sygn.: DOLiS-033-163/15/MM/ 37584 stanowczo zaoponował przeciwko rozstrzyganiu o ograniczaniu konstytucyjnej zasady jawności postępowania sądowego oraz udostępnianiu danych osobowych stron postępowania, a zatem w kwestii prawa do ochrony prywatności osób biorących udział w postępowaniu w akcie wykonawczym.

[427] Projekty ustaw zawarte w drukach nr 2544, 2680 rozpatrywane były wspólnie, efektem tych prac było uchwalenie na pos. nr 87 dnia 20 lutego 2015 r. ustawy z dnia 20 lutego 2015 r. o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw (na dzień 27 maja 2015 r. niepublikowana w dzienniku urzędowym).

Pismem z dnia 5 listopada 2014 r.[428] na podstawie art. 191 ust. 1 pkt 1 Konstytucji RP oraz art. 16 ust. 2 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2001 r. Nr 14 poz. 147 z późn. zm.) Generalny Inspektor zwrócił się do Rzecznika Praw Obywatelskich o **rozważenie skierowania do Trybunału Konstytucyjnego wniosku o zbadanie zgodności przepisów § 12 ust. l pkt 8, ust 2 pkt 3, 4, 5 oraz § 14 rozporządzenia Ministra Sprawiedliwości z dnia 3 sierpnia 2001 r. w sprawie organizacji i zakresu działania rodzinnych ośrodków diagnostyczno-konsultacyjnych** (Dz. U. Nr 97, poz. 1063) z art. 51 ust. 1 i 5 oraz art. 47 w zw. z art. 31 ust. 3 Konstytucji RP oraz art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych.

GIODO wskazał, że przepisy rozporządzenia Ministra Sprawiedliwości z dnia 3 sierpnia 2001 r. w sprawie organizacji i zakresu działania rodzinnych ośrodków diagnostyczno - konsultacyjnych (Dz. U. Nr 97, poz. 1063), zwanego dalej rozporządzeniem, wydane na podstawie art. 84 ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2001 r., Nr 97, poz. 1063, ze zm) regulują działalność rodzinnych ośrodków diagnostyczno-konsultacyjnych, w tym realizację przez te placówki zadań diagnostyczno-opiniodawczych, poradnictwa i konsultacji oraz pozyskiwanie i przechowywanie przez ośrodki danych osobowych zawartych w dokumentacji obejmującej m.in. „alfabetyczny wykaz osób badanych" (§ 12 ust 1 pkt 8 rozporządzenia) oraz „teczkach spraw kierowanych do ośrodka" zawierających „dane personalne osób, których dokumentację zawierają (§ 12 ust. 2 pkt 3), „protokoły działań merytorycznych, w szczególności przeprowadzonych wywiadów, testów, obserwacji, porad, mediacji i innych" (§ 12 ust. 2 pkt 4), „kopie sporządzonych opinii" (§ 12 ust. 2 pkt 5), „kopie rachunków wystawionych z tytułu prowadzonych działań" (§ 12 ust. 2 pkt 6)".

Zagadnienia objęte powyższą regulacją niewątpliwie stanowią materię ustawową. Ponadto dokumentacja sporządzana przez ośrodki diagnostyczno-konsultacyjne, może obejmować dane tzw. wrażliwe (szczególnie chronione), wymienione w art. 27 ust. 1 (np. dane o stanie zdrowia, nałogach, życiu seksualnym, dane dotyczące skazań). W świetle powołanych uwarunkowań konstytucyjnych, jak również wobec jednoznacznego brzmienia art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, który to przepis uzależnia dopuszczalność przetwarzania – wymienionych w art. 27 ust. 1 tejże ustawy – danych szczególnie chronionych od istnienia zezwolenia na takie przetwarzanie w przepisach

[428] DOLiS-035-1717/14.

szczególnych innej ustawy, stwarzającej przy tym pełne gwarancje ochrony tych danych, zasady oraz zakres przetwarzanych w związku z działalnością ośrodków diagnostyczno-konsultacyjnych danych osobowych muszą być określone w normach ustawowych. W celu zapewnienia wspomnianych gwarancji normy ustawowe powinny w sposób precyzyjny określać zasady postępowania z danymi osobowymi, w tym zasady ich udostępniania oraz podmioty uprawnione i odpowiedzialne za proces gromadzenia i przechowywania danych osobowych. Rozporządzenie mogłoby natomiast jedynie konkretyzować regulacje ustawowe, nie zaś stanowić samoistną podstawę dla przetwarzania danych tzw. szczególnie chronionych.

Prawo do ochrony prywatności i prawo do ochrony danych osobowych są prawami osobistymi gwarantowanymi przez Konstytucję RP (art. 47 i art. 51), dlatego też w wystąpieniu tym GIODO wskazał także na stanowisko Trybunału Konstytucyjnego dotyczące analizy relacji między przepisami art. 47 i art. 51 Konstytucji RP, służących – zdaniem Trybunału - ochronie tej samej wartości.[429] Także w wyroku o sygn. K 41/02 Trybunał Konstytucyjny podniósł:: „Wzajemna relacja między tymi dwoma przepisami Konstytucji polega (...) na tym, że autonomia informacyjna (por. art. 51 Konstytucji) jest jednym z komponentów prawa do prywatności w szerokim, przyjętym w art. 47 Konstytucji tego słowa znaczeniu" i pełni przede wszystkim funkcje gwarancyjne[430].

Ograniczenie w zakresie korzystania z wyżej opisanych praw: prawa do ochrony życia prywatnego i decydowania o swoim życiu osobistym - jakim jest niewątpliwie przymusowe podawanie informacji w ramach przeprowadzonych przez ośrodki badań i testów - wymaga regulacji rangi ustawowej (art. 31 ust. 3 Konstytucji RP), z uwzględnieniem stanowiska Trybunału Konstytucyjnego w tym zakresie[431].

Generalny Inspektor podniósł, że stosowanie przepisów kwestionowanego rozporządzenia prowadzi w praktyce do naruszenia innego konstytucyjnie i ustawowo

---

[429] Np. w wyrokach o sygn K 33/08 i SK 40/01.

[430] Por. wyrok o sygn. SK 40/01: „Prawo do ochrony danych osobowych [art. 51 Konstytucji] stanowi niewątpliwie szczególny instrument ochrony tych interesów podmiotu, które są związane z ochroną życia prywatnego. Prawo to jest więc wyspecjalizowanym środkiem ochrony tych samych wartości, które są chronione za pośrednictwem art. 47 Konstytucji"; podobnie wyrok o sygn. K 33/08: „art. 51 Konstytucji stanowi szczególny środek ochrony tych samych wartości, które chronione są za pośrednictwem art. 47 Konstytucji").

[431] Zgodnie ze stanowiskiem Trybunału Konstytucyjnego, z uzasadnienia postanowienia z dnia 31 stycznia 2007 roku (sygn. akt S 1/2007): *„Z zasady wyłączności regulacji ustawowej w sferze praw i wolności wynika, iż Parlament nie może w dowolnym zakresie „cedować" funkcji prawodawczych na organy władzy wykonawczej. Zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nienależące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej. Także art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki."*

gwarantowanego prawa jednostki: prawa do kontroli procesu przetwarzania danych zawartych w dokumentacji sporządzanej i przechowywanej przez rodzinne ośrodki diagnostyczno-konsultacyjne. Generalnemu Inspektorowi sygnalizowano przypadki odmawiania osobom, których dane dotyczą lub przedstawicielom ustawowym tych osób, dokumentacji badań przeprowadzanych przez rodzinne ośrodki diagnostyczno–konsultacyjne. W sprawach sygnalizowanych Generalnemu Inspektorowi wskazywano, że kierownicy rodzinnych ośrodków diagnostyczno-konsultacyjnych odmawiają osobom, wobec których badania były przeprowadzane, udostępniania prowadzonej dokumentacji, a zatem brak jest gwarancji dostępu do danych osobowych w niej zgromadzonych. Jako uzasadnienie takiej odmowy podawano np. że „dokumentacja taka jest materiałem roboczym służącym biegłym do opracowania opinii i czytelnym tylko dla nich, poza tym testy psychologiczne mogą być udostępniane wyłącznie specjalistom"[432].

Przepisy kwestionowanego rozporządzenia wzbudzają wątpliwości i zastrzeżenia nie tylko osób, których dane dotyczą. Z pism kierowanych do Generalnego Inspektora przez prezesów sądów[433] wynika bowiem, że istotnym problemem dotyczącym ośrodków diagnostyczno-konsultacyjnych jest również rozstrzyganie, kto w konkretnych przypadkach jest podmiotem posiadającym status administratora danych (tj. decyduje o celach i środkach przetwarzania danych osobowych), a tym samym ponosi odpowiedzialność za przetwarzanie danych osobowych zawartych w dokumentacji. Oczywiście wątpliwości takie dodatkowo pogłębiają trudności w wykonywaniu przez osoby uprawnione swojego prawa do kontroli przetwarzania danych osobowych, gdyż często nie jest wiadome, do którego z podmiotów należy zwrócić się w celu realizacji tego prawa. Kwestia, kto w odniesieniu do konkretnej dokumentacji i zgromadzonych w niej danych osobowych, jest podmiotem za nią odpowiedzialnym sprawia trudności nawet samym sądom (prokuraturom) zlecającym

---

[432] W reakcji na zgłaszane Generalnemu Inspektorowi przypadki naruszeń prawa do ochrony danych osobowych organ skierował wystąpienie do Ministra Sprawiedliwości w marcu 2012 r. (treść wystąpienia wraz z udzieloną na nie odpowiedzią dostępne są pod adresem http://www.giodo.gov.pl/1520149/id_art/5039/j/pl/). W odpowiedzi na wystąpienie GIODO w lipcu 2012 r. Ministerstwo Sprawiedliwości potwierdziło, że obecna regulacja dotycząca funkcjonowania rodzinnych ośrodków diagnostyczno-konsultacyjnych może budzić wątpliwości i zapewniło, że w związku w związku z prowadzonymi wówczas pracami nad projektem założeń ustawy o zmianie ustawy postępowaniu w sprawach nieletnich i ustawy – Prawo o ustroju sądów powszechnych *„rozważy wprowadzenie do ustawy rozwiązań zmierzających do rozwiązania kwestii poruszonych w wystąpieniu Generalnego Inspektora Ochrony Danych Osobowych"*. Niestety powyższe deklaracje nie zostały spełnione, mimo że ustawa o postępowaniu w sprawach nieletnich została w dużym zakresie znowelizowana ustawą z dnia 30 sierpnia 2013 r. o zmianie ustawy o postępowaniu w sprawach nieletnich oraz niektórych innych ustaw (Dz. U. z 2013 r., poz. 1165).

[433] Korespondencja w sprawach prowadzonych pod sygnaturą Biura GIODO: DOLiS-035-1717/14 i DOLiS-035-1742/14.

przeprowadzenie opinii, oraz kierownikom ośrodków diagnostyczno-konsultacyjnych oraz sądom, przy których ośrodki te działają.

W ocenie Generalnego Inspektora u podstaw powyższych trudności, skutkujących w wielu przypadkach naruszeniem konstytucyjnie chronionych praw, leży brak regulacji na poziomie ustawowym podstawowych kwestii dotyczących zasad tworzenia i prowadzenia takiej dokumentacji oraz roli poszczególnych podmiotów w zakresie administrowania tą dokumentacją. Kwestie te powinny być w sposób jednoznaczny i precyzyjny przesądzone w przepisach rangi ustawowej, łącznie z zagwarantowaniem wprost, że osoba, której dokumentacja dotyczy, jest uprawniona do wglądu do tej dokumentacji. Takie rozwiązanie pozwoliłoby na realizację prawa do kontroli procesu przetwarzania danych osobowych zgromadzonych w zbiorze (zbiorach) jaki dokumentacja ta stanowi.

Problem wadliwości przepisów prawa regulujących działalność rodzinnych ośrodków diagnostyczno-konsultacyjnych został zgłoszony przez Prokuratora Generalnego Trybunałowi Konstytucyjnemu w lipcu 2013 r.[434] Toteż skierowanie do Trybunału Konstytucyjnego wniosku mającego na celu zbadanie zgodności przepisów kwestionowanego rozporządzenia Ministra Sprawiedliwości z normami konstytucyjnymi i ustawowymi dotyczącymi prawa do prywatności i ochrony danych osobowych w zakresie postulowanym przez Generalnego Inspektora, stworzyłoby możliwość ewentualnego połączenia przez Trybunał Konstytucyjny spraw obu wniosków, i tym samym dokonania wnioskowanej oceny w szybszym terminie.

Mając powyższe na uwadze GIODO wskazał, że obecna regulacja dotycząca funkcjonowania rodzinnych ośrodków diagnostyczno-konsultacyjnych w postaci aktu wykonawczego jest w jego ocenie niezgodna z Konstytucją RP i ustawą o ochronie danych osobowych, a jej stosowanie prowadzi w praktyce do istotnych naruszeń praw i wolności

[434] Sprawa Trybunału Konstytucyjnego o sygn.: U 6/13, na wniosek Prokuratora Generalnego z dnia 9 lipca 2013 r. o sygn.: PG VIII TKw 38/12, którym Prokurator Generalny m.in. wskazał, że rozporządzenie w sprawie organizacji i zakresu działania rodzinnych ośrodków diagnostyczno konsultacyjnych zostało wydane z przekroczeniem upoważnień ustawy o postępowaniu w sprawach nieletnich, a więc z naruszeniem art. 92 ust. 1 Konstytucji. W ocenie Prokuratora Generalnego, wydając powyższe rozporządzenie Minister Sprawiedliwości przekroczył granice upoważnienia ustawowego określonego w art. 84 § 3 ustawy o postępowaniu w sprawach nieletnich. Przekroczenie to polega na przyznaniu rodzinnym ośrodkom diagnostyczno - konsultacyjnym kompetencji do wydawania opinii w innych sprawach niż sprawy nieletnich, to jest w sprawach z zakresu prawa rodzinnego i opiekuńczego, np. w sprawach o rozwód bądź separację w kwestii ustalania kontaktów między rodzicami a małoletnimi dziećmi, mimo braku wyraźnych do tego ustawowych podstaw prawnych. W konsekwencji w ocenie Prokuratora Generalnego § 11 ust. 1 rozporządzenia Ministra Sprawiedliwości w sprawie organizacji i zakresu działania rodzinnych ośrodków diagnostyczno-konsultacyjnych oraz załącznik nr II do tego rozporządzenia są niezgodne z art. 84 § 3 ustawy o postępowaniu w sprawach nieletnich, a tym samym z art. 92 ust. 1 Konstytucji.

osób, których dane osobowe, są pozyskiwane i przechowywane przez rodzinne ośrodki diagnostyczno-konsultacyjne.

Generalny Inspektor po otrzymaniu od Państwowej Inspekcji Pracy informacji, że pracodawcy (administratorzy danych osobowych pracowników) przekazują zewnętrznym podmiotom (np.: świadczącym usługi z zakresu szkoleń w dziedzinie bezpieczeństwa i higieny pracy czy prowadzącym biura rachunkowe lub obsługi dokumentacji) przetwarzającym następnie dane pracowników zawarte w ich aktach osobowych, ewidencji czasu pracy oraz dokumentacji wynagrodzeń, bez wymaganej przepisami ustawy o ochronie danych osobowych podstawy prawnej kierował do tych pracodawców wystąpienia[435] o podjęcie stosownych działań mających na celu zapewnienie podstaw prawnych do takiego działamnia. Wskazał w swych pismach, że podmioty przetwarzające dane osobowe są obowiązane do stosowania przepisów ustawy o ochronie danych osobowych na każdym etapie przetwarzania tych danych, zarówno w sytuacji, gdy zbierają dane, przechowują je, czy też udostępniają. W świetle przepisów ustawy o ochronie danych osobowych do podstawowych obowiązków administratora danych należy spełnienie jednej z przesłanek legalności przetwarzania (w tym udostępniania) danych, które w odniesieniu do danych osobowych tzw. zwykłych określone zostały w art. 23 ust. 1 ustawy. Zastrzec należy, że dane szczególnie chronione, określone w art. 27 ust. 1 ustawy podlegają bardziej restrykcyjnej ochronie. Zgodnie z art. 27 wymienionej ustawy przetwarzanie powyższych danych jest co do zasady zabronione, a zasada ta doznaje wyjątków jedynie w przypadkach enumeratywnie wyliczonych w art. 27 ust. 2 ustawy[436].

---

[435] DOLiS-035-2097/14, DOLiS-035-2098/14.

[436] Art. 27. 1. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. 2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli: 1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych; 2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony; 3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora; 4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych; 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem; 6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie; 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem

GIODO wskazał, że w uzasadnionych przypadkach stosowną podstawą przekazania danych osobowych przez ich administratora innemu podmiotowi może być zawarta na piśmie pomiędzy tym podmiotem a administratorem danych umowa powierzenia przetwarzania danych, o której mowa w art. 31 wymienionej ustawy. Podmiot ten może przetwarzać dane wyłącznie w celu i zakresie przewidzianym w umowie. Umowa taka musi określać zakres i cel przetwarzania danych, które zostały powierzone. Podmiot, któremu przetwarzanie danych zostało powierzone na mocy art. 31 ustawy o ochronie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 – 39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy[437]. Podkreślenia wymaga, iż w zakresie przestrzegania tych przepisów podmiot ten ponosi odpowiedzialność jak administrator danych[438]. Ponadto jest on związany w swej działalności zakresem i celem przetwarzania w przedmiotowej umowie wyznaczonym. Może zatem przetwarzać dane wyłącznie w takim zakresie i celu, jaki został przewidziany w jej treści. Przedmiotem powierzenia przetwarzania danych osobowych może być przy tym zarówno kompleksowa obsługa procesu przetwarzania danych dla określonego celu, jak i jedynie tylko niektóre operacje na danych, jak np. ich przechowywanie czy

---

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. Ponadto, mocą art. 26 ust. 1 pkt 1-3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem (pkt 1), zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2 (pkt 2), merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (pkt 3).

[437] Tj. 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).

[438] Art. 31. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. 2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. 3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych. 4. W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, - co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

usuwanie. Powierzenie przetwarzania danych osobowych następuje bez konieczności uzyskiwania zgody osób, których dane dotyczą.

Administrator danych, zawierając umowę powierzenia danych, jest zobowiązany do koordynacji procesu jej wykonywania. Powierzenie przetwarzania danych osobowych, o którym mowa w art. 31 ustawy, nie oznacza też zmiany statusu administratora danych osobowych, tj. pozostaje on podmiotem decydującym o celach o środkach przetwarzania danych osobowych, natomiast podmiot prowadzący działalność w imieniu i na rzecz administratora danych nie ma możliwości jakiegokolwiek wykorzystania tychże danych do własnych celów, czy potrzeb.

Generalny Inspektor wskazał więc, iż aby przekazywanie danych osobowych innemu podmiotowi było legalne, konieczne jest istnienie ku temu odpowiedniej podstawy prawnej, - tj. spełnienia przesłanki z art. 23 ust. 1 lub art. 27 ust. 2 ustawy o ochronie danych osobowych lub zawarcie umowy powierzenia przetwarzania danych osobowych zgodnie z art. 31 ust. 1 tejże ustawy. Skorzystanie z ostatniego z wymienionych przepisów jest rozwiązaniem najczęściej spotykanym w przypadkach zlecania wykonywania określonych zadań pracodawcy podmiotom zewnętrznym, np. przeprowadzania szkoleń BHP lub obsługi księgowej. Powierzenie przetwarzania danych nie oznacza wyzbycia się statusu podmiotu decydującego o celach i środkach przetwarzania, nie oznacza innymi słowy zmiany administratora danych, czy możliwości przetwarzania danych przez podmiot, któremu powierzono dla jego własnych celów.

W swoich wystąpieniach GIODO zwracał również uwagę na obowiązek właściwego zabezpieczenia danych. Obowiązek ten wynika w szczególności z rozdziału 5 powołanej ustawy, jak i rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Na administratorze danych spoczywa 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. Innymi słowy art. 36 ust. 1 ustawy zobowiązuje każdego administratora danych do wprowadzenia takich środków oraz rozwiązań technicznych i organizacyjnych, które zapewnią danym osobowym, w konkretnych warunkach i okolicznościach przetwarzania,

skuteczną ochronę przed potencjalnymi zagrożeniami. Jak już wyżej wspomniano, również podmiot, któremu przetwarzanie danych zostało powierzone na mocy art. 31 ustawy o ochronie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć odpowiednie środki zabezpieczające zbiór danych.

Niewywiązanie się z obowiązku właściwego zabezpieczenia danych może w konsekwencji prowadzić do powstania odpowiedzialności karnej. Przepisy karne ustawy o ochronie danych osobowych dotyczące niedopełnienia obowiązków w zakresie właściwego zabezpieczenia danych osobowych poprzez użycie określeń „administrujący zbiorem", „administrujący danymi osobowymi", „obowiązany do ochrony danych osobowych" wskazują, kto może odpowiadać za właściwe zabezpieczenie danych osobowych. Sprawcą czynu z art. 51 lub 52 ustawy o ochronie danych osobowych może być, oprócz kierownika jednostki, również administrator bezpieczeństwa informacji lub inny pracownik danej jednostki odpowiedzialny za ochronę danych, jak również każda osoba przetwarzająca dane osobowe na podstawie upoważnienia administratora danych[439].

W określonych przypadkach można również rozważać odpowiedzialność dyscyplinarną lub porządkową z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2014 r. poz. 1502 z późn. zm.).

W odpowiedzi na tego typu wystąpienia GIODO otrzymywał wyjaśnienia dotyczące podjętych przez administratorów działań w celu usunięcia zasygnalizowanych nieprawidłowości[440].

W związku z uzyskaniem przez Generalnego Inspektora informacji o **upublicznieniu na stronie internetowej jednej z gmin danych osobowych w treści uchwały w sprawie uchwalenia miejscowego planu zagospodarowania przestrzennego** Generalny Inspektor skierował wystąpienie do tego podmiotu[441].

Zgodnie z art. 29 ust. 1 ustawy z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (t.j. Dz. U. z 2012 r. poz. 647 z pożn. zm.), uchwała rady gminy w sprawie uchwalenia planu miejscowego obowiązuje od dnia wejścia w życie w niej

---

[439] Art. 51. 1. 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. 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

[440] M.in. pismo jednej z gmin z dnia 27 czerwca 2014 r. o sygn.: SG.1420.2.2.2014.

[441] DOLiS-035-1027/14.

określonego, jednak nie wcześniej niż po upływie 14 dni od dnia ogłoszenia w dzienniku urzędowym województwa. Zgodnie natomiast z ust. 2 tego artykułu, uchwała, o której mowa w ust. 1, podlega również publikacji na stronie internetowej gminy.

Zdaniem organu do spraw ochrony danych osobowych jednakże, w aspekcie upublicznienia miejscowego planu zagospodarowania przestrzennego gminy, zakres przetwarzanych danych osobowych, w tym udostępnianych publicznie, w każdym procesie ich przetwarzania musi być adekwatny do jego przedmiotu i być niezbędny dla osiągnięcia określonego celu. Zgodnie z zasadami legalizmu, adekwatności przetwarzania danych w stosunku do celu ich przetwarzania i zasadą związania celem, zachowana powinna zostać równowaga pomiędzy dobrem osoby, której dane dotyczą, a interesem (w tym prawnie określonym) administratora danych[442]. Oznacza to, że administrator danych nie może przetwarzać, w tym udostępniać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem stopniu szczegółowości.

W przedmiotowej sprawie zastrzeżenia GIODO były tym bardziej uzasadnione, iż usunięcie personaliów osób prywatnych, czy też ich zanonimizowanie w ogłoszonej w BIP uchwale nie wpływa na czytelność dokonanego w ten sposób przekazu. Jednocześnie, stanowisko judykatury jednoznacznie potwierdza zastrzeżenia GIODO[443].

Odnośnie zaś zarządzenia wójta gminy w sprawie powierzenia pełnienia obowiązków dyrektora gminnego ośrodka kultury, które to zarządzenie obejmowało dane osobowe osoby, która pełni obowiązki dyrektora (imię i nazwisko oraz adres zamieszkania), jak i osoby na czas usprawiedliwionej nieobecności zastępowanej (imię i nazwisko), Generalny Inspektor wskazał, iż zgodnie z art. 15 ust. 1 ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych (tekst pierwotny: Dz. U. z 2008 r. Nr 223 poz. 1458 z poźn. zm.), niezwłocznie po przeprowadzonym naborze na stanowisko urzędnicze (w rozumieniu tej ustawy), w tym kierownicze stanowisko urzędnicze, informacja o wyniku naboru jest

---

[442] Stosownie bowiem do treści art. 26 ust. 1 pkt 1 i 3 ustawy o ochronie danych osobowych, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

[443] Np. wyrok Wojewódzkiego Sądu Administracyjnego z dnia 18 listopada 2009 r. w sprawie o sygn. akt II SA/Wa 1177/08, w uzasadnieniu którego sąd podniósł, iż *„usunięcie personaliów osób prywatnych, czy też ich zanonimizowanie w ogłoszonej w BIP uchwale (...) nie wpływa na czytelność dokonanego w ten sposób przekazu. W tym przypadku treść aktu administracyjnego nie traci waloru informacyjnego, albowiem wynika z niej kto, kiedy i w jakiej sprawie publicznej zajął określone stanowisko. Podstawowym celem BIP jest powszechne informowanie o sprawach publicznych i w tym przypadku cel ten został zrealizowany. Prezentowanie odmiennego poglądu pozostaje w sprzeczności z konstytucyjnymi gwarancjami wolności i praw obywatela."*

upowszechniana przez umieszczenie na tablicy informacyjnej w jednostce, w której był przeprowadzony nabór, oraz opublikowanie w Biuletynie przez okres co najmniej 3 miesięcy. Zgodnie jednak z ustępem 2 tego artykułu, informacja, o której mowa w ust. 1, zawiera: 1) nazwę i adres jednostki; 2) określenie stanowiska; 3) imię i nazwisko wybranego kandydata oraz jego miejsce zamieszkania w rozumieniu przepisów Kodeksu cywilnego; 4) uzasadnienie dokonanego wyboru albo uzasadnienie nierozstrzygnięcia naboru na stanowisko.

Zgodnie natomiast z art. 25 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2014 r. poz. 121 z poźn. zm.) miejscem zamieszkania osoby fizycznej jest miejscowość, w której osoba ta przebywa z zamiarem stałego pobytu. Jedynie więc takie informacje należy publikować.

W odpowiedzi na ww. wystąpienie Generalny Inspektor otrzymał zapewnienie o dokonaniu przeglądu informacji znajdujących się na stronie internetowej gminy, pod kątem usunięcia wszystkich danych osobowych, których zamieszczenie było zbędne[444].

Celem wystąpienia Generalnego Inspektora skierowanego w dniu 18 czerwca 2014 r. do innej gminy, było spowodowanie rezygnacji przez nią ze stosowania **formularza wniosku o udostępnienie informacji publicznej, w którym wymagane jest podanie imienia i nazwiska, adresu, numeru PESEL oraz numeru telefonu wnioskodawcy pomimo, iż wnioskodawca ma możliwość otrzymania odpowiedzi na adres poczty elektronicznej**, ponadto za pomocą tego formularza wnioskodawcy obligowani byli do udzielania zgody na przetwarzanie danych w celu realizacji przedmiotowego wniosku[445].

W swym wystąpieniu organ wskazał, iż z punktu widzenia przepisów ustawy o ochronie danych osobowych przetwarzanie danych osobowych jest dopuszczalne m.in. wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. 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.

Przetwarzanie danych osobowych zwykłych jest dopuszczalne m.in. wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, natomiast danych szczególnie chronionych m.in. wówczas, gdy przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i

[444] Pismo gminy z dnia 27 czerwca 2014 r. o sygn.: SG.1420.2.2.2014.
[445] DOLiS-035-1241/14.

stwarza pełne gwarancje ich ochrony. Podmioty publiczne natomiast działać mogą jedynie na podstawie i w granicach obowiązujących je przepisów prawa, w ramach kompetencji nadanych im tymi przepisami.

Stosownie do przepisów ustawy 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 niniejszej ustawie. Informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej lub centralnym repozytorium, jest udostępniana na wniosek[446].

W sytuacji natomiast istnienia przesłanki legalności przetwarzania danych innej, niż zgoda osoby, której dane dotyczą[447] dodatkowe pozyskiwanie zgody osoby, której dane dotyczą na przetwarzanie dotyczących jej danych jest zbędne.

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. To bowiem 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, 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.[448]

---

[446] Art. 10 ust. 1 ustawy o dostępie do informacji publicznej.

[447] Tj. określonej w art. 23 ust. 1 pkt 1 i art. 27 ust. 2 pkt 1 ustawy.

[448] Por. wyrok Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 10 maja 2012 r. sygn. IISAB/Łd 46/12, czy wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 24 lutego 2012 r. sygn. IV SAB/GI 75/11.

Mając na uwadze powyższe, GIODO zwrócił się do wójta gminy o wnikliwe przeanalizowanie zgłoszonych niniejszym pismem uwag i podjęcie niezbędnych działań mających na celu zmianę opisanej powyżej praktyki. W aktualnym stanie prawnym brak jest bowiem uzasadnienia dla stosowania formularza sugerującego wymóg podania określonych danych osobowych. Innymi słowy, ponieważ postępowanie w sprawie udostępnienia informacji publicznej ma charakter odformalizowany, wniosek taki może być złożony w dowolnie wybranej formie, bez konieczności stosowania konkretnego wzoru formularza, jak i brak jest podstaw wyznaczających konieczność przetwarzania określonych danych osobowych wnioskodawcy.

W odpowiedzi gmina poinformowała o usunięciu kwestionowanego formularza ze strony internetowej gminy[449].

Generalny Inspektor wystosował także wiele wystąpień dotyczących **nieuzasadnionego zatrzymywania dowodów osobistych przez podmioty, które w zamian za oferowane usługi udostępnienia infrastruktury, czy określonych przedmiotów, żądały pozostawienia tego dokumentu[450], jako zabezpieczenia wywiązania się z umowy.** Kwestionowana praktyka stosowana jest coraz powszechniej, i budzi sprzeciw organu do spraw ochrony danych osobowych, w każdym przypadku, tj. niezależnie od tego czy związana jest np. z wypożyczeniem sprzętu ośrodka sportowego, przyczepy, audioprzewodnika muzeum państwowego czy końcówki kompresora na stacji benzynowej – bo i taką praktykę GIODO napotkał w swej działalności.

Szczególne zaniepokojenie Generalnego Inspektora dotyczy stosowania takich działań przez podmioty publiczne, które powinny sobie zdawać sprawę, iż zgodnie z art. 79 pkt 2 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2010 r. Nr 167, poz. 1131 z późn. zm.), kto zatrzymuje bez podstawy prawnej cudzy dowód osobisty podlega karze ograniczenia wolności albo karze grzywny. Poprzednio zaś, nieuprawnione zatrzymanie dowodu tożsamości było sprzeczne z przepisami 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.). Artykuł 33 ustawy o ewidencji ludności i dowodach osobistych zabraniał zatrzymywania dowodu osobistego, chyba że takie uprawnienie przyznają odrębne przepisy. Kto zaś zatrzymuje bez podstawy prawnej dowód osobisty, zgodnie z art. 55 pkt 2 wspomnianej ustawy, podlegał karze ograniczenia wolności albo karze grzywny.

[449] Pismo gminy z dnia 3 lipca 2014 r. o sygn.: OrIV.1333.18.2014
[450] Np. DOLiS-035-2008/14, DOLiS-035-4480/13, DOLiS-035-3623/13, DOLiS-035-3748/13.

Generalny Inspektor wskazywał w tych sprawach, iż dokonywanie przez administratora danych rzetelnej analizy, czy i dla jakich celów przetwarzanie, w tym pozyskiwanie, określonego rodzaju danych powinno następować na etapie poprzedzającym dokonywanie każdej operacji na danych osobowych. 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 zaś, 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[451].

Przetwarzanie danych z dowodu osobistego nie będzie zatem niezgodne z prawem, jeśli przetwarzanie wszystkich danych pochodzących z tego dokumentu będzie znajdowało stosowną podstawę prawną, a zarazem o ile nie będzie prowadziło do gromadzenia danych w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są przetwarzane. Przetwarzanie danych nie może odbywać się w sposób, który narusza obowiązujące przepisy prawa. O ile natomiast sam sposób pozyskiwania danych osobowych jest z punktu widzenia ustawy o ochronie danych osobowych obojętny[452], to czynność przetrzymywania dokumentu tożsamości budzi już uzasadnione zastrzeżenia pod kątem prawidłowego dopełnienia zasad legalności, adekwatności i celowości działań administratorów danych[453].

W odpowiedziach na powyższe wystąpienia podmioty informowały o odstąpieniu od kwestionowanej praktyki, przyjęciu rozwiązań polegających na pobieraniu opłat zwracanych

[451] Tak np. w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r.; sygn. akt II SA/Wa 917/2005.

[452] 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.

[453] Art. 23 ustawy i art. 26 ust. 1 pkt 1-4 ustawy o ochronie danych osobowych.

wraz ze zwrotem sprzętu, bądź polegających ograniczeniu przetwarzania danych do wglądu, ewentualnie spisania cech dokumentu, nie zaś utrwalaniu całej jego treści.

Powyższe zastrzeżenia, choć dotyczyły przetwarzania danych osobowych związanych z zatrzymywaniem dowodów osobistych należy też odnieść do podobnych sytuacji związanych z zatrzymywaniem chociażby praw jazdy, paszportów czy różnego rodzaju legitymacji.

Inna grupa wystąpień dotyczyła powszechnej nieprawidłowości, polegającej na **nieukrywaniu w masowej wysyłce korespondencji elektronicznej adresów e-mailowych adresatów**[454].

Na wstępie przypomniano administratorom danych osobowych, którzy praktykowali takie działania, iż adres poczty elektronicznej należy traktować jako informację, która potencjalnie może być daną osobową, ale z uwzględnieniem wszelkich okoliczności występujących w konkretnym przypadku. Każdorazowo decydujące znaczenie dla ewentualnego uznania ich za dane osobowe będzie miała możliwość identyfikacji pośredniej określonego użytkownika, a więc identyfikacja z wykorzystaniem dodatkowych informacji będących w posiadaniu administratora danych lub innych osób[455].

Osoba, do której skierowana jest korespondencja przesyłana także do innych odbiorców, co do zasady, nie powinna mieć możliwości zapoznawania się z danymi pozostałych adresatów wiadomości. Administrator danych osobowych jest bowiem zobowiązany do przestrzegania przepisów ustawy o ochronie danych osobowych, w tym art. 36 ust. 1 w/w ustawy. W przypadku wysyłania korespondencji do większej liczby osób należy dbać o to, aby dane osobowe nie były udostępniane wszystkim adresatom wiadomości, albowiem nie są oni uprawnieni do pozyskiwania baz adresów e-mailowych innych odbiorców komunikatu, - nie posiadają ku temu przesłanki legalności przetwarzania danych, o której mowa w art. 23 ust. 1 ustawy.

---

[454] Np. DOLiS-035-1245/14, DOLiS-0351238/14

[455] Zgodnie bowiem z treścią art. 6 ust. 1 ustawy o ochronie danych osobowych 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). Stosownie do ust. 3 powołanego przepisu, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Adres poczty elektronicznej będzie stanowił daną osobową, o ile nie będą zachodziły przesłanki z wyżej przytoczonego art. 6 ust. 3 ustawy. Kryterium ułatwiającym uznanie adresu e-mail za daną osobową może być w szczególności jego treść.

Generalny Inspektor podniósł też, iż zgodnie z brzmieniem art. 51 ustawy o ochronie danych osobowych udostępnianie przez administratora zbioru danych (np. spółkę) albo osoby obowiązane do ochrony danych osobowych (pracowników) osobom do tego nieupoważnionym jest czynem karalnym zagrożonym przynajmniej karą grzywny[456].

Dlatego też za dobrą praktykę należy uznać przesyłanie wiadomości skierowanej do większej ilości odbiorców w taki sposób, aby żaden z nich nie mógł zapoznać się z adresami poczty elektronicznej innych adresatów wiadomości.

W odpowiedziach, jako najczęstszy powód zaistniałych okoliczności wskazywano omyłkę, czy brak doświadczenia pracownika określonego podmiotu, stosownymi zaś czynnościami wewnętrznymi zapobiegano tego rodzaju (ewentualnym) dalszym naruszeniom przepisów ustawy o ochronie danych osobowych.

Podobną do powyżej omawianej grupy wystąpień dotyczących **upubliczniania danych osobowych stanowiły wystąpienia kierowane do parafii rzymskokatolickich, które w swej działalności w różny sposób ujawniały dane osobowe osób związanych z kościołem**[457].

Takie ujawnienia związane były np. z umieszczeniem na drzwiach kościoła danych osobowych w postaci imienia i nazwiska, miejscowości oraz kwoty przekazanej podczas kolędy, publikacji w parafialnym periodyku danych osobowych darczyńców (nazwisk, pierwszych liter imienia oraz nazw ulic) składających ofiary na dzwony do kościoła parafialnego oraz danych osobowych (imienia i nazwiska oraz miejscowości) osób przystępujących do sakramentów (chrztu, pierwszej komunii świętej, ślubu), czy w związku z publikacją pozycji książkowej zawierającą dane osobowe mieszkańców (w szczególności imienia i nazwiska, daty urodzenia i zawodu).

Sprawy te były istotnymi m.in. z tego powodu, iż dotyczyły także tzw. danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, tj. przekonań religijnych lub filozoficznych, przynależności wyznaniowej. Przetwarzanie takich danych dopuszczalne jest jedynie w przypadkach wskazanych w ustawie[458].

---

[456] Zgodnie z postanowieniem art. 201 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz.U. 2013 poz. 1030) ewentualna odpowiedzialność za wyżej określone działania może spoczywać, obok pracowników spółki, na osobach kierujących spółką, która występuje w roli administratora danych osobowych zobowiązanego do przestrzegania zasad przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa.

[457] DOLiS-035-102/14, DOLiS-44015/14, DOLiS-440-15/14.

[458] Tj. stosownie do norm wynikających z art. 27 ust. 2 pkt 1-10 ustawy o ochronie danych osobowych.

Generalny Inspektor wskazywał, iż administrator danych, przetwarzający dane osobowe osób zamieszkujących daną parafię, pozyskanych na potrzeby Kościoła, zobowiązany jest do przestrzegania wszelkich, tym bardziej podstawowych zasad przetwarzania danych osobowych wyrażonych w ustawie o ochronie danych osobowych[459]. Opublikowanie, czy ujawnienie danych osobowych w sposób, który umożliwia zapoznanie się z nimi osobom nieupoważnionym w opinii Generalnego Inspektora nie może odbywać się bez podstawy prawnej, zwłaszcza w sposób naruszający interes osób, których dane dotyczą.

W przedstawionych sprawach konieczne jest także uwzględnienie przepisów określających obowiązek właściwego zabezpieczenia danych.[460]

Trudno jednocześnie zakładać, że przedmiotowe sprawy dotyczyły osób innych, niż członkowie kościoła. Jednocześnie brak było podstaw do przyjęcia, że udostępnienie danych osobowych w określony powyżej sposób mogło być niezbędne z punktu widzenia jakichkolwiek statutowych działań kościoła. Przetwarzanie danych ujawniających przekonania religijne jest natomiast dopuszczalne jeżeli jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych[461].

Kościół Katolicki korzysta z niezależności, a przepisy prawa gwarantują mu jako instytucji możliwość posługiwania się wewnętrznie ustalonym prawem. Zgodnie bowiem z art. 2 ustawy z dnia 17 maja 1989 roku (t. j. Dz. U. z 2013 r. poz. 1169) o stosunku Państwa - do Kościoła Katolickiego w Rzeczypospolitej Polskiej, Kościół rządzi się w swych sprawach własnym prawem, swobodnie wykonuje władzę duchowną i jurysdykcyjną oraz zarządza swoimi sprawami. Nie zmienia to jednak w opinii Generalnego Inspektora faktu, iż Kościół Katolicki i inne związki wyznaniowe zobowiązane są do przestrzegania powszechnie

[459] Określonych w art. 26 ust. 1 ustawy o ochronie danych osobowych.

[460] Obowiązek ten wynika zarówno z przepisów 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. z 2004 r. Nr 100 poz. 1024).

[461] Zgodnie z art. 27 ust. 2 pkt 4 ustawy o ochronie danych osobowych.

obowiązujących, dotyczących ochrony danych osobowych przepisów prawa[462], które nie są wyłączone na mocy zawartych umów, czy odrębnych przepisów dotyczących autonomii kościołów w Polsce.

Z napływających w tych sprawach odpowiedzi na wystąpienia, GIODO pozyskał informacje o zaprzestaniu kwestionowanych działań.

8.2. Działalność informacyjna.

Do działalności informacyjnej GIODO, podobnie jak w latach ubiegłych, wykorzystywane były sprawdzone już w wieloletniej działalności Urzędu, różnorodne kanały komunikacyjne, takie jak:

- media tradycyjne i elektroniczne,
- strona internetowa GIODO (na bieżąco aktualizowana i uzupełniana),
- 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 mediami),
- indywidualne spotkania z interesantami podczas dyżurów pełnionych przez Zastępcę GIODO i pracowników departamentów,
- publikacje książkowe (powstające przy udziale GIODO i pracowników Biura),
- Infolinia (czynna od poniedziałku do piątku, w godzinach pracy Biura).

[462] Należy wspomnieć o treści art. 3a ust. 2 ustawy o ochronie danych osobowych, zgodnie z którym ustawy nie stosuje się (za wyjątkiem przepisów art. 14-19 i art. 36 ust. 1) do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. z 1984 r. Nr 5 poz. 24 z późn. zm.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą. Przy czym, jak zasygnalizowano w orzecznictwie, w uzasadnieniu wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 marca 2007 r. (sygn. akt II SA/Wa 1933/06): *„nie można przyjmować, że właściwym do oceny istotności naruszeń praw i wolności, o których mowa w art. 3a ust. 2 u.o.d.o. powinien być GIODO, bowiem wśród kompetencji GIODO nie ma uprawnień do badania istotności naruszeń praw i wolności (...)"*. Z pewnością jednak badanie istotności naruszeń praw i wolności może odbywać się w drodze postępowania sądowego. Stąd też Generalny Inspektor zauważa, że publikowanie danych osobowych w ramach działalności dziennikarskiej może prowadzić do istotnego naruszenia praw i wolności osób, których dane dotyczą.

8.2.1. Współpraca ze środkami masowego przekazu

Jednym z elementów podnoszenia świadomości społeczeństwa w sprawach związanych z prawem do prywatności i ochrony danych osobowych jest systematyczne informowanie obywateli o przysługujących im prawach w tym zakresie oraz o działalności GIODO jako eksperta w dziedzinie ochrony danych. W tym celu Generalny Inspektor Ochrony Danych Osobowych podejmuje działania służące zwiększeniu widoczności organu m.in. w prasie i w opinii publicznej, co owocuje zarówno wzrostem zaufania publicznego do instytucji, jak i zwiększonym zaangażowaniem obywateli w ochronę przysługujących im praw.

1. Stałe kontakty z mediami.

Wzorem lat ubiegłych, w 2014 r. organ do spraw ochrony danych osobowych, realizując cele informacyjno-edukacyjne, kontynuował stałą współpracę z mediami polegającą na przekazywaniu do publikacji materiałów,, w tym wydanych decyzji, wystąpień, sygnalizacji GIODO, jak i gotowych do druku opracowań konkretnych zagadnień z zakresu ochrony danych osobowych. Taka współpraca była prowadzona zarówno z prasą codzienną o zasięgu ogólnopolskim, przede wszystkim z „Rzeczpospolitą" „Dziennikiem Gazetą Prawną" „Pulsem Biznesu" i „Gazetą Wyborczą", jak i ogólnopolskimi pismami branżowymi, m.in. „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", „Tina" czy „Świat Kobiety". W 2014 r. stała współpraca GIODO ze stacjami telewizyjnymi i radiowymi, m.in. z Informacyjną Agencją Radiową, Polskim Radiem Jedynką, Trójką Polskim Radiem, Polskim Radiem 24, Radiem TOK FM, Radiem dla Ciebie, TVP INFO, Telewizją Polsat, Superstacją czy TVN24, zaowocowała emisją wielu programów o tematyce ochrony danych osobowych. Materiały dotyczącej tej problematyki zamieszczały również współpracujące z GIODO agencje informacyjne - PAP, KAI i Newseria.

W 2014 r. w prasie, radiu, telewizji i Internecie opublikowanych lub wyemitowanych zostało ponad **100** materiałów prasowych o tematyce ochrony danych. Przeważająca ich część 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 i 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 aplikacji mobilnych,
- funkcjonowanie portali społecznościowych w kontekście wykorzystywania danych osobowych ich użytkowników,
- odmowa udostępnienia informacji publicznej, zwłaszcza przez jednostki samorządu terytorialnego, z powołaniem się na ochronę danych osobowych,
- upublicznianie przez jednostki samorządu terytorialnego w BIP uchwał, decyzji czy protokołów z danymi osobowymi osób fizycznych,
- wykorzystywanie danych osobowych na potrzeby marketingu, ze szczególnym uwzględnieniem jednej z jego form, tj. telemarketingu,
- możliwość dochodzenia swoich praw w związku z otrzymywaniem niechcianej korespondencji e-mailowej lub sms-owej, czyli tzw. spamu,
- wyłudzanie danych osobowych dla celów przestępczych, czego konsekwencją jest kradzież tożsamości,
- udostępnianie nieznanym podmiotom przez osoby, których dane dotyczą, szczegółowych informacji na swój temat i zagrożenia z tym związane,
- zabezpieczanie danych osobowych przez firmy i instytucje, w tym placówki opieki zdrowotnej,
- możliwość stosowania monitoringu wizyjnego przez instytucje inne, niż ustawowo upoważnione,
- kompetencje GIODO w stosunku do kościołów i związków wyznaniowych w kontekście apostazji, czyli występowania z tych instytucji,
- upublicznianie przez parafie list zawierających dane osobowe darczyńców wraz z ofiarowaną kwotą czy osób niesprzątających kościoła,

- przetwarzanie danych osobowych zarówno lekarzy, jak i pacjentów przez portale oceniające lekarzy,
- żądanie pozostawienia dowodu osobistego lub innego dokumentu potwierdzającego tożsamość w zastaw za wypożyczany sprzęt, np. narty, łyżwy, kajaki czy audio przewodniki,
- skanowanie dowodów osobistych przez podmioty, z którymi osoby fizyczne zawierają różnego rodzaju umowy,
- zbieranie podpisów pod petycjami czy listami poparcia oraz zabezpieczanie takich dokumentów,
- upublicznianie danych osobowych dłużników, np. na drzwiach wejściowych do budynków.

Na pytania dziennikarzy GIODO w 2014 r. udzielił ponad **400** odpowiedzi.

3. Wywiady i wystąpienia.

Tematyka wywiadów radiowych i telewizyjnych oraz udzielonych 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 dziennikarzy budziła też możliwość bezpiecznego korzystania z urządzeń mobilnych czy portali internetowych, zwłaszcza społecznościowych. Wśród innej, poruszanej w rozmowach problematyki, związanej z wykorzystaniem nowoczesnych technologii wymienić można: Internet przedmiotów, monitorowanie pracowników czy instalowanie monitoringu wizyjnego.

Niesłabnącym zainteresowaniem mediów cieszyła się również reforma prawa regulującego ochronę danych osobowych na poziomie Unii Europejskiej, zarówno w kontekście zakresu planowanych zmian, jak i ich wpływu na prawodawstwo krajowe oraz działalność instytucji i przedsiębiorców z obszaru całej UE.

Kolejnymi komentowanymi i wyjaśnianymi przez GIODO zagadnieniami były: profilowanie bezrobotnych, przetwarzanie tzw. danych retencyjnych, zwłaszcza w kontekście wyroków Trybunału Sprawiedliwości Unii Europejskiej oraz Trybunału Konstytucyjnego, propozycja utworzenia przez Ministerstwo Finansów rejestru dłużników posiadających zaległości w zakresie danin publicznych, propozycja zapewnienia ministrowi sprawiedliwości dostępu do akt postępowań sądowych, montowanie wideorejestratorów w prywatnych

- przetwarzanie danych osobowych zarówno lekarzy, jak i pacjentów przez portale oceniające lekarzy,
- żądanie pozostawienia dowodu osobistego lub innego dokumentu potwierdzającego tożsamość w zastaw za wypożyczany sprzęt, np. narty, łyżwy, kajaki czy audio przewodniki,
- skanowanie dowodów osobistych przez podmioty, z którymi osoby fizyczne zawierają różnego rodzaju umowy,
- zbieranie podpisów pod petycjami czy listami poparcia oraz zabezpieczanie takich dokumentów,
- upublicznianie danych osobowych dłużników, np. na drzwiach wejściowych do budynków.

Na pytania dziennikarzy GIODO w 2014 r. udzielił ponad **400** odpowiedzi.

3. Wywiady i wystąpienia.

Tematyka wywiadów radiowych i telewizyjnych oraz udzielonych 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 dziennikarzy budziła też możliwość bezpiecznego korzystania z urządzeń mobilnych czy portali internetowych, zwłaszcza społecznościowych. Wśród innej, poruszanej w rozmowach problematyki, związanej z wykorzystaniem nowoczesnych technologii wymienić można: Internet przedmiotów, monitorowanie pracowników czy instalowanie monitoringu wizyjnego.

Niesłabnącym zainteresowaniem mediów cieszyła się również reforma prawa regulującego ochronę danych osobowych na poziomie Unii Europejskiej, zarówno w kontekście zakresu planowanych zmian, jak i ich wpływu na prawodawstwo krajowe oraz działalność instytucji i przedsiębiorców z obszaru całej UE.

Kolejnymi komentowanymi i wyjaśnianymi przez GIODO zagadnieniami były: profilowanie bezrobotnych, przetwarzanie tzw. danych retencyjnych, zwłaszcza w kontekście wyroków Trybunału Sprawiedliwości Unii Europejskiej oraz Trybunału Konstytucyjnego, propozycja utworzenia przez Ministerstwo Finansów rejestru dłużników posiadających zaległości w zakresie danin publicznych, propozycja zapewnienia ministrowi sprawiedliwości dostępu do akt postępowań sądowych, montowanie wideorejestratorów w prywatnych

samochodach i udostępniania nagrań Policji oraz w Internecie, a także doręczanie korespondencji sądowej przez Polską Grupę Pocztową.

Ponadto GIODO niejednokrotnie udzielał wywiadów poświęconych wyciekom danych osobowych, bezpiecznemu korzystaniu ze zbliżeniowych kart płatniczych, a także dopuszczalności tworzenia przez przedsiębiorców profili osobowych klientów.

W 2014 r. GIODO udzielił blisko **230** wywiadów.

4. Konferencje prasowe.

W związku z potrzebą nagłośnienia niektórych wydarzeń lub upublicznienia stanowiska GIODO w istotnych, dla ochrony danych osobowych sprawach, GIODO w 2014 r. zorganizował **8** konferencji prasowych. Poświęcone one były:

- obchodom VIII Dnia Ochrony Danych Osobowych w Polsce i w Brukseli (28 stycznia 2014 r. w Warszawie oraz 21 stycznia 2014 r. w Brukseli),
- funkcjonowaniu tzw. Karty Warszawiaka oraz Karty Małego Warszawiaka, podczas której GIODO poinformował, że mimo iż w jego opinii, wymiana danych między warszawskim ratuszem, ZTM i Ministerstwem Finansów dokonywana na potrzeby wydawania tych kart, jest bezprawna, nie wstrzyma ich wydawania (21 lutego 2014 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 4. edycji programu, a także problemy związane z przetwarzaniem danych osobowych uczestników gier on-line, ze szczególnym uwzględnieniem dzieci i młodzieży (29 maja 2013 r.),
- podstawowym zasadom ochrony danych osobowych, a także zagrożeniom, jakie dla ochrony danych i prywatności stanowi rozwój nowych technologii. Omówione zostały zasady bezpiecznego korzystania z aplikacji mobilnych, a także zagrożenia, jakie są związane z upowszechnianiem się Internetu przedmiotów. GIODO uczulał, by nie zapominać, jak wiele cyfrowych śladów pozostawiamy chociażby korzystając ze smartfona, biletu elektronicznego czy dokonując płatności kartą. Konferencja prasowa odbyła się w związku z IV Dniami Otwartymi GIODO (Trójmiasto, 23 czerwca 2014 r.),

- podpisaniu porozumienia GIODO z Uniwersytetem Jagiellońskim (Kraków, 12 czerwca 2014 r.).

Ponadto w 2014 r. GIODO – jako ekspert i gość honorowy – uczestniczył w konferencjach prasowych zorganizowanych przez współpracujące z Biurem instytucje. Dotyczyły one:

- sposobów, przy użyciu których przedsiębiorcy powinni chronić informacje i dane osobowe przed ich utratą. Z przedstawionych podczas konferencji badań, przeprowadzonych przez PricewaterhouseCoopers (PwC), wynika bowiem, że europejskie przedsiębiorstwa, zwłaszcza średniej wielkości, mają problem z właściwym zarządzaniem posiadanymi informacjami, przez co narażone są na ryzyko ich utraty. Wprawdzie świadomość konieczności zabezpieczania danych rośnie, lecz stosowane w tym celu metody i środki są stosunkowo słabe, co powoduje, że wykradane lub bezpowrotnie tracone są ogromne ilości informacji. GIODO, komentując wyniki badań wskazywał, że bezpieczeństwo informacyjne zawsze jest uzależnione od kontekstu, w którym dana firma bądź organizacja działają. Jak mówił, każdy przedsiębiorca powinien dokonać oceny ryzyka, by wiedzieć, które dane i w jaki sposób zabezpieczać. Organizatorem konferencji i zleceniodawcą badań była firma Iron Mountain (16 kwietnia 2014 r.),
- zjawiska kradzieży tożsamości możliwej ze względu na naszą niefrasobliwość i brak dbałości o własne dane osobowe, jak np. wyrzucanie dokumentów na śmietnik. Podczas konferencji zaprezentowano wyniki badań dotyczących świadomości i zachowań związanych z zabezpieczaniem danych osobowych przez osoby fizyczne, zarówno w świecie realnym, jak i wirtualnym. GIODO radził, jak chronić dane osobowe i swoją tożsamość, podkreślając, jak dużo zależy od nas samych w walce o ich bezpieczeństwo. Zwracał uwagę, że o właściwym niszczeniu dokumentów zawierających dane osobowe należy pamiętać zarówno przy pozbywaniu się materiałów papierowych, jak i tych zapisanych na nośnikach informatycznych. Organizatorem konferencji była firma Fellowes – realizująca od 2005 r., przy wsparciu GIODO, kampanię edukacyjną „Nie daj się okraść, chroń swoją tożsamość" (28 października 2014 r.).

5. Akcje informacyjno-promocyjne.

a) Dzień Ochrony Danych Osobowych

Z okazji obchodów Dnia Ochrony Danych Osobowych tradycyjnie, zarówno w Polsce, jak i w Brukseli, zorganizowane zostały konferencje prasowe GIODO (28 stycznia 2014 r. w Warszawie oraz 21 stycznia 2014 r. w Brukseli).

W ramach obchodów, wzorem lat ubiegłych, odbył się panel dyskusyjny „Aplikacje mobilne" zorganizowany przez GIODO oraz redakcję „Dziennika Gazety Prawnej" (16 stycznia 2014 r., siedziba Redakcji), którego zapis na łamach Gazety opublikowany został 7 lutego 2014 r.

Po raz kolejny tematy poruszane w czasie obchodów odbiły się dzięki mediom szerokim echem, co z pewnością przekłada się na lepszą edukację i osób, których dane dotyczą, i tych, którzy dane przetwarzają.

b) Debaty

Nagłośnianiu istotnych, z punktu widzenia ochrony danych osobowych, zagadnień służą również organizowane w mediach od lat debaty. W roku sprawozdawczym GIODO był współorganizatorem debaty w Redakcji „Dziennika Gazety Prawnej", która odbyła się 3 grudnia 2014 r. Jej temat brzmiał „Prawo do informacji a prawo do prywatności". Uczestniczyli w niej eksperci, naukowcy i praktycy zajmujący się ochroną danych osobowych i dostępem do informacji publicznej: dr Arwid Mednis, radca prawny, partner w Kancelarii Wierzbowski Eversheds, dr Grzegorz Sibiga, reprezentujący Instytut Nauk Prawnych PAN - oraz Radę Informatyzacji przy MAiC, Paweł Litwiński z Instytutu Allerhanda, Krzysztof Izdebski, ekspert z Pozarządowego Centrum Dostępu do Informacji Publicznej oraz Marlena Sakowska-Baryła, radca prawny z Urzędu Miasta Łodzi oraz dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych.

c) Wakacyjna kampania informacyjna

W 2014 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 poradnik poświęcony temu, jak chronić dane osobowe w różnych sytuacjach, w jakich znajdujemy się podczas wakacji. GIODO udzielał praktycznych wskazówek, 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 podawanie naszych danych osobowych różnym podmiotom, np. biurom podróży, przewoźnikom, hotelom, sklepom internetowym jest bezpieczne. Ponadto GIODO wyjaśniał, czy używanie opcji „zapamiętaj hasło" jest bezpieczne, czy po zakończeniu korzystania z serwisów internetowych zawsze powinniśmy się wylogowywać, o czym musimy pamiętać, korzystając z telefonów komórkowych czy smartfonów. Radził też, jak postępować, gdy zgubimy telefon albo smartfon bądź zostanie on skradziony.

Poradnik został zamieszczony na stronie internetowej GIODO, a linki do niego znalazły się nie tylko na stronach internetowych ponad 30 innych urzędów i instytucji biorących udział w tej akcji. Tematy poruszane w poradniku GIODO zostały bowiem 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 2014 r. za jej pośrednictwem udzielono wyjaśnień ponad **12 tysiącom** osób. Jej utworzenie 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. Ponieważ na potrzeby obsługującej całą Polskę Infolinii uruchomiony jest w Biurze tylko jeden numer telefonu, GIODO otrzymuje wiele skarg od osób, które nie są w stanie się dodzwonić.

7. Newsletter.

W 2014 r. GIODO kontynuował wydawanie Newslettera, dostarczanego wszystkim, wyrażającym chęć jego otrzymywania poprzez zarejestrowanie się za pośrednictwem strony internetowej GIODO. W 2014 r. przygotowanych zostało **6** jego numerów.

Newsletter stanowi źródło najświeższych informacji o działalności Generalnego Inspektora Ochrony Danych Osobowych (GIODO), 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 inicjatywa Generalnego Inspektora Ochrony Danych Osobowych podjęta w 2012 r. 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 pracy lub 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 23-25 czerwca 2014 r. zorganizowane zostały w Trójmieście **IV Dni Otwarte GIODO.** Generalny Inspektor Ochrony Danych Osobowych, we współpracy m.in. z Uniwersytetem Gdańskim, Prezydentem Miasta Gdyni, Prezydentem Miasta Gdańska oraz Regionalną Izbą Gospodarczą Pomorza i Pracodawcami Pomorza, przygotował szereg wydarzeń, w tym konferencję naukową poświęconą ochronie prywatności w świecie nowych technologii komunikacyjnych, a także cykl spotkań seminaryjno-szkoleniowych dla administracji publicznej i przedsiębiorców.

Pierwszym wydarzeniem, które odbyło się w ramach IV Dnia Otwartego GIODO, była konferencja szkoleniowa dla pracowników Urzędu Miasta Gdyni 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. Odbyła się też Konferencja Naukowa pt. **„Ochrona prywatności w świecie nowych technologii komunikacyjnych"** zorganizowana przez Biuro GIODO wspólnie z Wydziałem Prawa i Administracji Uniwersytetu Gdańskiego. Głównymi tematami Konferencji była prywatność w świecie Internetu przedmiotów, ochrona danych osobowych w inteligentnych sieciach energetycznych oraz informatyzacja służby zdrowia. Podczas trwania obu wydarzeń czynne były stoiska informacyjne, przy których eksperci z Biura GIODO udzielali bezpłatnych porad i informacji z zakresu ochrony danych osobowych oraz rozdawali materiały edukacyjno–informacyjne Biura GIODO.

Z kolei 24 czerwca 2014 r. – tradycyjnie z okazji Dni Otwartych GIODO – odbyło się Śniadanie z przedsiębiorcami poświęcone bezpieczeństwu przetwarzania danych osobowych,

zorganizowane wspólnie z firmą Iron Mountain. 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 i IV Dzień Otwarty GIODO stał się okazją, by tego typu wydarzenie zorganizować poza stolicą.

W tym samym dniu miała miejsce konferencja szkoleniowa dla pracowników Urzędu Miejskiego w Gdańsku, jednostek organizacyjnych miasta oraz przedstawicieli Gdańskiego Obszaru Metropolitarnego, której tematy związane były z aktualnymi problemami stosowania ochrony danych osobowych przez organy samorządu terytorialnego oraz VI Międzynarodowa Konferencja Naukowo-Techniczna „Technologie morskie dla obronności i bezpieczeństwa" - zorganizowana jako projekt towarzyszący XIII Bałtyckim Targom Militarnym BALT MILITARY EXPO. Podczas tego wydarzenia Generalny Inspektor Ochrony Danych Osobowych wygłosił wystąpienie pt. „Wykorzystanie danych z systemów eMaritime do potrzeb bezpieczeństwa morskiego, a ochrona prywatności osób". eMaritime są to systemy elektronicznego zarządzania elementami gospodarki morskiej przez wszystkie podmioty uczestniczące w całym łańcuchu logistycznym, na który składają się port i instytucje go obsługujące, firmy trudniące się załadunkiem, kontrahenci, pasażerowie, marynarze, itd. Rozbudowane systemy eMaritime umożliwiają zawieranie umów pomiędzy uczestnikami rynku morskiego i niejednokrotnie są też połączone z systemami służącymi, np. do zarządzania kryzysowego. Powoduje to, że dane w nich gromadzone są jednocześnie danymi z instytucji publicznych i rejestrów publicznych oraz danymi, które pozyskiwane są od podmiotów prywatnych. Mamy więc do czynienia z klasycznym przykładem łączenia wielu baz danych w rękach jednego podmiotu, którym czasem bywa port, czasem Urząd Morski, a czasem inna instytucja publiczna. Dlatego zadaniem GIODO tak ważna jest świadomość zagrożeń ochrony danych przetwarzanych w tym systemie.

Konferencja szkoleniowa z udziałem członków Regionalnej Izby Gospodarczej Pomorza i Pracodawcami Pomorza w Gdańskim Parku Naukowo-Technicznym, która poświęcona była aktualnym problemom z zakresu ochrony danych osobowych, w tym propozycjom nowych rozwiązań w projekcie ustawy o ułatwieniu wykonywania działalności gospodarczej oraz nowym rozwiązaniom projektu Rozporządzenia Parlamentu Europejskiego i Rady o ochronie danych, zakończyła program wydarzeń zaplanowanych na ten dzień.

Ostatnim punktem IV Dnia Otwartego GIODO w Trójmieście były warsztaty pt. **„Zwiększanie świadomości w zakresie ochrony danych wśród pracowników**

zatrudnionych w krajach Unii Europejskiej", podsumowujące projekt realizowany przez Generalnego Inspektora Ochrony Danych Osobowych we współpracy z organami ochrony danych osobowych z Chorwacji, Czech i Bułgarii, w ramach programu Leonardo da Vinci - oraz konferencja szkoleniowa dla sędziów Sądu Okręgowego w Gdańsku z zakresu ochrony danych osobowych w działalności sądów powszechnych.

8.2.3. Publikacje.

W ramach Projektu Partnerskiego Leonardo da Vinci "Zwiększanie świadomości w zakresie ochrony danych osobowych wśród pracowników zatrudnionych w krajach Unii Europejskiej", finansowanego przez Komisję Europejską w ramach programu „Uczenie się przez całe życie", organy ochrony danych z Polski, Czech, Bułgarii i Chorwacji opracowały publikację **„Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników"**. Przewodnik skierowany jest do osób fizycznych podejmujących zatrudnienie lub pracujących w jednym z krajów uczestniczących w projekcie. W ramach projektu eksperci reprezentujący cztery organy ochrony danych: Biuro Generalnego Inspektora Ochrony Danych Osobowych z Polski, Biuro Ochrony Danych z Republiki Czeskiej, Agencję Ochrony Danych Osobowych z Chorwacji oraz Komisję Ochrony Danych Osobowych z Republiki Bułgarii przeanalizowali aktualne problemy związane z zatrudnieniem i przedstawili wybrane zalecenia w zakresie ochrony danych i prywatności.

8.2.4. Szkolenia podmiotów zewnętrznych.

W ramach prowadzonej działalności edukacyjnej w 2014 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 2014 r. zwróciły się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o przeprowadzenie szkolenia znalazły się: Kancelaria Senatu, Urząd Ochrony Konkurencji i Konsumentów, Centralne Biuro Antykorupcyjne, Państwowa Inspekcja Pracy, Komenda Główna Policji, Laboratorium Kryminalistyczne Komendy Stołecznej Policji, Centrum Operacji Specjalnych – Dowództwo Komponentów Wojsk Specjalnych, Warszawska Opera Kameralna, Warszawski Uniwersytet Medyczny, Krajowa Rada Doradców Podatkowych, Krajowa Rada Radców Prawnych, Prokuratura Okręgowa w Warszawie, Rządowe Centrum Legislacji, Sąd Okręgowy w Gdańsku, Okręgowe Izby

Radców Prawnych w Białymstoku, Bydgoszczy, Gorzowie Wielkopolskim, Kaliszu, Katowicach, Kielcach, Koszalinie, Krakowie, Legnicy, Lublinie, Łodzi, Olsztynie, Opolu, Poznaniu, Rzeszowie, Szczecinie, Toruniu, Warszawie i Zielonej Górze, Ministerstwa: Sportu i Turystyki, Sprawiedliwości, Spraw Zagranicznych, Administracji i Cyfryzacji, Gospodarki, Spraw Wewnętrznych, a także Urząd Marszałkowski Województwa Śląskiego, Urząd Miejski w Wejherowie, oraz Urzędy Miast: Gdańska, Gdyni, Rzeszowa, Krakowa oraz m.st. Warszawy.

Niektóre szkolenia miały ogólnopolski zasięg, jak szkolenie realizowane w ramach IV edycji ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli".

W sumie w 2014 r. przeprowadzono **64 szkolenia** 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 wykład dla studentów Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego, podczas którego przedstawiciel GIODO omawiał zagadnienia z zakresu bezpieczeństwa baz danych w praktyce aptecznej w ramach przedmiotu Opieka Farmaceutyczna, czy udział zastępcy GIODO w szkoleniu dla przedstawicieli Komendy Wojewódzkiej Policji w Olsztynie (28.10.2014), w którym udział wzięli komendanci wszystkich komend i jednostek policji w województwie, osoby zajmujące się w tych placówkach ochroną danych osobowych, głównie administratorzy bezpieczeństwa informacji, a także przedstawiciele Centralnego Biura Śledczego (CBŚ) i Wyższej Szkoły Policji w Szczytnie – w sumie ponad 150 osób. Jedną z najważniejszych kwestii poruszaną na tym spotkaniu, była praktyka wzywania na świadków przedstawicieli Biura GIODO w związku z toczącymi się postępowaniami o przestępstwo naruszenia ochrony danych osobowych, w celu dokonania kwalifikacji prawnej popełnionych czynów oraz wydawania wiążących opinii dotyczących tych przestępstw. Tymczasem to administratorzy bezpieczeństwa informacji (ABI) w poszczególnych komendach powinni służyć fachową pomocą funkcjonariuszom prowadzącym postępowania w sprawach związanych z naruszeniem przepisów karnych z ustawy o ochronie danych osobowych.

Na uwagę zasługuje także szkolenie z zakresu ochrony danych osobowych przeprowadzone 27 października 2014 r. przez Generalnego Inspektora Ochrony Danych Osobowych w Krajowej Izbie Doradców Podatkowych. Uczestniczyli w nim członkowie

Krajowej Rady Doradców Podatkowych, w tym Przewodniczący Zarządów Regionalnych Oddziałów, Przewodniczący Wyższego Sądu Dyscyplinarnego, Przewodniczący Sądu Dyscyplinarnego, Przewodniczący Krajowej Komisji Rewizyjnej, a także Rzecznik Dyscypliny Krajowej Izby Doradców Podatkowych. Szkolenie było nagrywane w celu udostępnienia doradcom podatkowym, po uprzednim zalogowaniu się do systemu mDoradca.

W formule szkolenia przebiegało także spotkanie w Starogardzkim Klubie Biznesu – Związku Pracodawców w Starogardzie Gdańskim, z przedstawicielami administracji samorządowej, Prezydentem Miasta Starogard Gdański, naczelnikami i pracownikami Urzędu Skarbowego, Komendy Policji i przedsiębiorców (22.10.2014). Tematem spotkania była „Ochrona danych osobowych – stan, stosowanie oraz rozwiązania w przyszłym prawie krajowym oraz Unii Europejskiej".

Niektóre ze szkoleń miały formę wideokonferencji, jak to zorganizowane przez GIODO we współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie. Słuchaczami wykładu on-line pt. „Świat wirtualny a rzeczywisty. Wyzwania i zagrożenia w Internecie. Czy czujesz się bezpieczny? – jak rozmawiać z dziećmi i młodzieżą o ich problemach i bezpieczeństwie w wirtualnym świecie" (26.03.2014) byli dyrektorzy szkół, pracownicy ośrodków doskonalenia nauczycieli, konsultanci i doradcy metodyczni, nauczyciele i uczniowie szkół, które w minionym roku sprawozdawczym 2013 przystąpiły do kolejnej edycji programu edukacyjnego „Twoje dane – twoja sprawa (...)".

8.2.5. Konkursy.

W analizowanym 2014 r. Generalny Inspektor Ochrony Danych Osobowych był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

1. Konkurs GIODO i MAiC na aplikację mobilną.

Generalny Inspektor Ochrony Danych Osobowych wspólnie z Ministerstwem Administracji i Cyfryzacji zorganizował konkurs na aplikację mobilną przyjazną prywatności, którego celem było zachęcenie młodych twórców aplikacji mobilnych do przestrzegania zasad ochrony danych osobowych. Patronem konkursu była Fundacją Bezpieczna Cyberprzestrzeń Przedmiotem pracy konkursowej było stworzenie aplikacji zapewniającej wysoki standard ochrony danych osobowych, poprzez zastosowanie odpowiednich środków i procedur technicznych oraz organizacyjnych. W konkursie zwyciężyła aplikacja opracowana

przez dwuosobowy zespół z Politechniki Warszawskiej (aplikacja „SkyDe"), II miejsce zajął zespół studentów z Wojskowej Akademii Technicznej (aplikacja „Secure WALLET"), natomiast na III miejscu uplasowała się aplikacja „Interaktywny UEP" opracowana przez studentów z Uniwersytetu Ekonomicznego w Poznaniu. Prezentacja aplikacji przez zwycięskie zespoły oraz uroczystość wręczenia nagród przez Generalnego Inspektora Ochrony Danych Osobowych odbyła się podczas Konferencji „Security Case Study 2014", zorganizowanej w dniach 26-27 listopada 2014 r. w Warszawie przez Fundację Bezpieczna Cyberprzestrzeń, patrona konkursu.

2. Konkurs na esej dotyczący zagadnień z zakresu ochrony danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych po raz kolejny był organizatorem konkursu dla studentów prawa oraz studentów kierunku administracja na esej dotyczący zagadnień z zakresu ochrony danych osobowych. Przedmiotem IV edycji konkursu było przygotowanie pracy na temat monitorowania studentów podczas sesji egzaminacyjnej. Uczestnicy konkursu mieli za zadanie ustalić, czy uczelnia miała prawo – w przypadku podanym w kazusie – wykorzystywać nagrania z kamer zamontowanych w sali egzaminacyjnej. Partnerem merytorycznym konkursu dla studentów była kancelaria prawna PricewaterhouseCoopers Legal Szurmińska-Jaworska sp.k. Spośród nadesłanych na Konkurs prac, Generalny Inspektor Ochrony Danych Osobowych wyłonił laureatów, którzy otrzymali nagrody rzeczowe oraz nagrody specjalne w postaci nieodpłatnych praktyk w Biurze GIODO.

3. Konkurs dla uczniów na komiks lub animację na temat ochrony prywatności i danych osobowych.

Generalny Inspektor zorganizował konkurs dla uczniów szkół podstawowych, gimnazjów i szkół ponadgimnazjalnych objętych ogólnopolskim programem edukacyjnym Generalnego Inspektora Ochrony Danych Osobowych „Twoje dane-twoja sprawa. Skuteczna ochrona danych osobowych – inicjatywa skierowana do uczniów i nauczycieli". Celem konkursu było zachęcenie dzieci i młodzieży do zainteresowania się problematyką ochrony prywatności i danych osobowych poprzez twórcze przedstawienie swoich przemyśleń na ten temat oraz wyłonienie laureatów wśród uczniów szkół, którzy wykażą się wiedzą i kreatywnością z zakresu tej tematyki. Przedmiotem oceny były prace opowiadające krótką historię w formie komiksu lub animacji komputerowej. Przeprowadzenie konkursu zostało poprzedzone warsztatami, zorganizowanymi przy współpracy z Ośrodkiem Edukacji

Informatycznej i Zastosowań Komputerów, który jest partnerem programu edukacyjnego Generalnego Inspektora. Laureaci konkursu wraz z opiekunami wzięli udział w seminarium podsumowującym program edukacyjny w roku szkolnym 2013/2014, podczas którego wręczono nagrody. Dodatkowo, fragmenty lub całe prace laureatów i innych wybranych uczestników konkursu zostały zaprezentowane na wystawie podczas ww. seminarium, jak również na stronie internetowej GIODO.

4. Konkurs dla szkół i ośrodków doskonalenia nauczycieli.

Już po raz drugi Generalny Inspektor Ochrony Danych Osobowych zorganizował konkurs dla szkół i ośrodków doskonalenia nauczycieli w ramach ogólnopolskiego programu edukacyjnego „Twoje dane - twoja sprawa", aby promować najciekawsze inicjatywy mające na celu upowszechnienie wiedzy o ochronie danych osobowych i prawa do prywatności wśród uczniów i nauczycieli. Przedmiotem oceny były działania podjęte przez uczestników programu oraz partnerów metodycznych w ramach IV edycji programu. Główną nagrodę – Złote Pióro Programu otrzymała Szkoła Podstawowa z Oddziałami Integracyjnymi im. Powstańców Wielkopolskich w Nowych Skalmierzycach. Wśród nagrodzonych inicjatyw były m.in. gra planszowa „Bezpiecznie w sieci", gra „Skoczek" przeprowadzona z udziałem dzieci na sali gimnastycznej, debata międzyszkolna i sieć współpracy szkół w ramach programu, lekcje na temat ochrony danych osobowych, autorskie scenariusze zajęć dla najmłodszych opracowane na podstawie baśni oraz współpraca szkół ze środowiskiem lokalnym, a także zajęcia dla uczniów z rodzicami przy tworzeniu awatar-ów.

8.2.6. Projekty i programy.

W roku sprawozdawczym 2014, Biuro GIODO kontynuowało swój udział w projektach. Pierwszy z projektów stanowił projekt finansowany ze środków Unii Europejskiej w ramach Programu Leonardo da Vinci (LdV) będącego częścią Programu „Uczenia się przez całe życie" *(Lifelong Learning Programme)*. W 2014 r. kontynuowany był projekt PHAEDRA finansowany ze środków Komisji Europejskiej, którego realizacja rozpoczęła się w 2013 r. Ponadto w analizowanym roku sprawozdawczym 2014 rozpoczęła się realizacja projektu ARCADES, również finansowanego ze środków Komisji Europejskiej.

Innego rodzaju projektem, którego realizację kontynuowano w 2014 r. był krajowy program edukacyjny, który GIODO organizuje od 2009 r. pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.

1. Unijne projekty partnerskie

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 było 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 było podjęcie 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 przez GIODO w ramach projektu partnerskiego LdV, która ukazała się w 2011 r. Pozytywne opinie pochodzące od różnych grup odbiorców, głównie przedsiębiorców oraz przedstawicieli sektora edukacji, ugruntowały przekonanie o potrzebie opracowania kolejnego przewodnika, - tym razem skierowanego do pracowników podejmujących zatrudnienie w jednym z krajów uczestniczących w projekcie.

W związku z tym organy ochrony danych osobowych z Polski, Czech, Bułgarii i Chorwacji opracowały publikację pt. „Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników". Przewodnik skierowany jest do osób fizycznych podejmujących zatrudnienie lub pracujących w jednym z krajów uczestniczących w projekcie. W ramach projektu eksperci reprezentujący cztery organy ochrony danych: Biuro Generalnego Inspektora Ochrony Danych Osobowych z Polski, Biuro Ochrony Danych z Republiki Czeskiej, Agencję Ochrony Danych Osobowych z Chorwacji oraz Komisję Ochrony Danych Osobowych z Republiki

Bułgarii przeanalizowali aktualne problemy związane z zatrudnieniem i przedstawili wybrane zalecenia w zakresie ochrony danych i prywatności. Oficjalna prezentacja Przewodnika odbyła się podczas warsztatów podsumowujących projekt partnerski, które odbyły się w dniu 25 czerwca 2014 r. w Gdańsku.

Wspomniany projekt ukierunkowany był 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 przyczynił się do wzmocnienia współpracy między europejskimi organami ochrony danych osobowych, które brały w nim udział.

2. 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 był współfinansowany przez Unię Europejską (Dyrekcję Generalną Sprawiedliwości – DG Justice) w ramach programu Prawa Podstawowe i Obywatelstwo (Fundamental Rights and Citizensship – „Action grants")[463]. 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 było 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 etapem projektu było przygotowanie rekomendacji zmierzających do poprawy tej sytuacji. W efekcie

[463] JUST/2012/FRAC/AG/2761.

projekt przyczynił się do poprawy współpracy i koordynacji działań między wszystkimi zainteresowanymi stronami w zapewnieniu rzeczywistej ochrony danych osobowych.

W ramach projektu PHAEDRA partnerzy projektu przeprowadzili cykl konsultacji z przedstawicielami organów ochrony danych osobowych. Konsultacje miały na celu przeanalizowanie potrzeb i oczekiwań europejskich organów ochrony danych osobowych w zakresie działań, jakie można podjąć celem wzmocnienia współpracy i koordynacji między poszczególnymi organami ochrony danych osobowych, rzecznikami prywatności czy innymi instytucjami zajmującymi się ochroną prywatności na poziomie ogólnoświatowym oraz zidentyfikowania barier we współpracy miedzy tymi organami. Ustalenia poczynione w trakcie spotkań miały znaczący wpływ na dalszy kierunek prac w ramach projektu PHAEDRA.

W dniu 24 stycznia 2014 r. w Brukseli odbyło się spotkanie partnerów tego projektu z przedstawicielami europejskich organów ochrony danych osobowych i rzeczników prywatności oraz innych instytucji zajmujących się ochroną prywatności na poziomie ogólnoświatowym. W spotkaniu, które odbywało się pod patronatem 7. Międzynarodowej Konferencji „Komputery, Prywatność i Ochrona Danych" („Computers, Privacy and Data Protection – CPDP 2014"), uczestniczył Generalny Inspektor Ochrony Danych Osobowych. Spotkanie poświęcone było omówieniu dotychczasowych rezultatów projektu PHAEDRA - oraz dyskusji nad dalszym kierunkiem działań, które przyczynią się do wzmocnienia współpracy między poszczególnymi europejskimi i światowymi instytucjami ochrony danych osobowych i prywatności.

Przypomnienia wymaga, że 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. Natomiast kolejne, drugie z kolei warsztaty, które miały miejsce w Skopje 6 maja 2014 r., przebiegały pod hasłem „Wyzwania i bariery współpracy i koordynacji działań pomiędzy organami ochrony danych osobowych". Trzecia edycja warsztatów projektu PHAEDRA pt. „Rozporządzenie UE o ochronie danych osobowych w perspektywie udoskonalenia współpracy na poziomie regionalnym pomiędzy organami ochrony danych osobowych (DPAs), rzecznikami ds. ochrony prywatności (PCs) oraz organami ds. egzekwowania ochrony danych osobowych i prywatności (PEAs)", miały miejsce w Seulu, w dniach 17-18 czerwca 2014 r. Ostatnie, 4. warsztaty w ramach tego dwuletniego projektu, zorganizowane zostały przez Generalnego Inspektora Ochrony Danych Osobowych na

Mauritiusie, podczas 36. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, 12-18 października 2014 r.

Międzynarodowa Konferencja **„Egzekwowanie prywatności: wnioski z obecnego wdrażania i perspektywy na przyszłość"**, zorganizowana przez Generalnego Inspektora Ochrony Danych Osobowych w Krakowie (12.12.2014), zamykała projekt PHAEDRA prezentacją rezultatów końcowych i dyskusją na temat szerszej współpracy i koordynacji działań między organami ochrony danych osobowych, rzecznikami prywatności i organami wdrażania prawa prywatności. Konferencja skierowana była do organów ochrony danych osobowych, decydentów, przedstawicieli środowisk akademickich, organizacji pozarządowych oraz mediów[464].

3. Projekt ARCADES.

W 2014 r. rozpoczęła się realizacja projektu ARCADES pn. „Wprowadzenie kwestii związanych z ochroną danych oraz prywatności do szkół w Unii Europejskiej" (Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union – ARCADES) finansowanego ze środków Komisji Europejskiej w ramach programu Prawa podstawowe i Obywatelstwo (Fundamental Rights and Citizenship), koordynowanego przez Dyrekcję Generalną ds. Sprawiedliwości (DG Justice). Biuro Generalnego Inspektora Ochrony Danych Osobowych jest koordynatorem projektu, zaś partnerami są: Vrije Universiteit Brussel z Belgii, Rzecznik Ochrony Danych Republiki Słowenii oraz Krajowy Urząd ds. Ochrony Danych i Wolności Informacji z Węgier.

Inspiracją dla tego przedsięwzięcia był ogólnopolski program edukacyjny GIODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", który spotkał się z ogromnym zainteresowaniem szkół i ośrodków metodycznych kształcenia nauczycieli w Polsce. Generalny Inspektor podjął wówczas decyzję o przeniesieniu idei tego programu na grunt europejski. Celem projektu ARCADES jest wprowadzenie do programu nauczania w szkołach państw Unii Europejskiej treści związanych z ochroną danych osobowych oraz prywatności. Adresatami projektu są nauczyciele edukujący na poziomie podstawowym i średnim, których zadaniem jest kształtowanie świadomych i odpowiedzialnych postaw wśród dzieci i młodzieży w wieku 6-19 lat. Pośród różnych działań zaplanowanych na czas trwania projektu, konsorcjum

[464] Więcej informacji na temat projektu PHAEDRA, dostępnych jest na stronie http://www.phaedra-project.eu.

przewiduje opracowanie skutecznych metod edukowania dzieci i młodzieży w temacie prawa do prywatności i ochrony danych osobowych oraz wydanie publikacji prezentującej wyniki projektu, pomoce dydaktyczne, scenariusze lekcji oraz inne materiały pomocne w nauczaniu.

Spotkanie inaugurujące projekt ARCADES odbyło się 7 listopada 2014 r. w siedzibie jednego z partnerów projektu - Vrije Universiteit Brussel w Brukseli. Natomiast jesienią 2015 r. w Polsce, Słowenii i na Węgrzech zostaną zorganizowane dwudniowe seminaria dla nauczycieli, podczas których uczestnicy otrzymają niezbędną wiedzę o ochronie danych osobowych wraz z kompletem materiałów do opracowania scenariuszy lekcji z tego zakresu. W ramach projektu zaplanowano bowiem konkurs na najlepszy scenariusz lekcji poświęconej ochronie prywatności i danych osobowych. Zwycięskie scenariusze zostaną zaprezentowane podczas konferencji kończącej projekt, która odbędzie się w 2016 r. Brukseli z okazji X Dnia Ochrony Danych Osobowych.

Na zakończenie projektu przygotowana zostanie publikacja dla nauczycieli, w której znajdą się materiały z zakresu prawa do prywatności i ochrony danych osobowych oraz wybrane scenariusze lekcji. Wspomniana publikacja zostanie rozpowszechniona wśród organów ochrony danych w Unii Europejskiej.

Czas trwania projektu wynosi 18 miesięcy (3.XI.2014 r. – 3.05.2016 r.).

4. Krajowy program edukacyjny.

W 2014 r. kontynuowany był ogólnopolski program edukacyjny „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", skierowany do tych, którzy uważają, że odpowiednia wiedza i kształtowanie nawyków w obszarze ochrony prywatności i danych osobowych umożliwi dzieciom i młodzieży sprawne, odpowiedzialne i bezpieczne funkcjonowanie we współczesnym świecie. 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 – mogli 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.

Do programu mogą przystąpić szkoły podstawowe, gimnazja i szkoły ponadgimnazjalne oraz placówki doskonalenia nauczycieli.

W rezultacie do 4. edycji programu w roku 2013/2014 zgłosiło się 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.

Dla uczestników programu rok 2014 rozpoczął się organizacją obchodów VIII Dnia Ochrony Danych Osobowych. W ramach tego święta szkoły zorganizowały konkursy dla uczniów (wiedzy, plastyczne, multimedialne), quizy, apele, lekcje otwarte, pogadanki, przedstawienia autorskie z zakresu ochrony danych osobowych z udziałem dzieci i młodzieży oraz wizyty w urzędach miast i gmin, prokuraturze i sądzie, ośrodkach zdrowia, komisariatach Policji, bankach i innych instytucjach w celu poinformowania o Dniu. Ponadto uczniowie wzięli udział w grach miejskich, piknikach oraz happeningach, podczas których rozdawali przechodniom ulotki informujące o prawie każdego do prywatności i dotyczących go danych osobowych. Natomiast w szkołach uczniowie redagowali okolicznościowe gazetki tematyczne, plakaty, na tablicach ogłoszeń, na szkolnych korytarzach, świetlicach i salach lekcyjnych pojawiły się informacje dotyczące obchodzonego w Polsce 28 stycznia Europejskiego Dnia Ochrony Danych Osobowych, a przez szkolny radiowęzeł emitowano audycje na ten temat.

Generalny Inspektor Ochrony Danych Osobowych we współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie zorganizował wykład on-line pt. „Świat wirtualny a rzeczywisty. Wyzwania i zagrożenia w Internecie. Czy czujesz się bezpieczny? – jak rozmawiać z dziećmi i młodzieżą o ich problemach i bezpieczeństwie w wirtualnym świecie". Słuchaczami wykładu byli dyrektorzy szkół, ośrodków doskonalenia nauczycieli, konsultanci i doradcy metodyczny, nauczyciele i uczniowie szkół, które przystąpiły do programu.

Natomiast w dniu 29 maja 2014 r. GIODO zorganizował seminarium podsumowujące - IV edycję programu realizowanego w latach 2013/2014, któremu towarzyszyła wystawa prac konkursowych w formie komiksów przygotowanych przez uczniów. Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych referatem pt. „Uczeń i jego awatar. Ochrona prywatności w grach MMORPG" rozpoczął sesję poświęconą prywatności w cyfrowym świecie, zaś zaproszeni goście w swych wystąpieniach podkreślili wysoką rangę działań edukacyjnych GIODO skierowanych do dzieci i młodzieży, dostrzegając ich rolę i

wartość w budowaniu kompetencji cyfrowych młodego pokolenia. Seminarium było także okazją do prezentacji działań zrealizowanych przez liderów IV edycji tego programu. Uczestnikom seminarium zaprezentowana została m.in. gra planszowa „Bezpiecznie w sieci", gra „Skoczek na sali gimnastycznej", oraz uliczna gra miejska „Na tacy poDANE".

W roku szkolnym 2014/2015 program był kontynuowany w formie V edycji. Szkolenie dla przedstawicieli szkół i ośrodków doskonalenia nauczycieli, które zostały zgłoszone do V edycji programu odbyło się w dniach 23-24 października 2014 r. w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie. Dwudniowe szkolenie miało na celu przygotowanie uczestników Programu „Twoje dane – twoja sprawa (...)" do prowadzenia zajęć z uczniami w szkołach podstawowych, gimnazjach i szkołach podstawowych na temat ochrony danych osobowych i prawa do prywatności, jak również przedstawicieli ośrodków doskonalenia nauczycieli do prowadzenia spotkań z nauczycielami i dyrektorami szkół w ramach programu. Podczas szkolenia uczestnicy otrzymali pakiety edukacyjne zawierające m.in. materiały informacyjne dotyczące zasad ochrony danych osobowych i przykładowe scenariusze lekcji oraz materiały promocyjne programu (plakaty, ulotki). Szkolenie zostało podzielone na część wykładową i warsztatową. W pierwszym dniu szkolenia zostały omówione główne idee programu, dobre praktyki w jego realizacji ogólne zasady ochrony danych osobowych w placówkach oświatowych oraz działania organizacji pozarządowych w obszarze edukacji dzieci i młodzieży na temat ochrony danych osobowych i prawa do prywatności. Wykłady poprowadzili eksperci Biura Generalnego Inspektora Ochrony Danych Osobowych oraz liderzy poprzednich edycji Programu, jak również przedstawiciele Fundacji Dzieci Niczyje i Fundacji Panoptykon. W części warsztatowej przedstawiciele Biura Generalnego Inspektora Ochrony Danych Osobowych, Ośrodka Edukacji Informatycznej i Zastosowań Komputerów oraz nauczyciele – liderzy programu, którzy realizują program od wielu lat z dużym sukcesem angażując przy tym całą społeczność szkolną oraz środowisko lokalne, prowadzili interesujące zajęcia wskazując na przykłady dobrych praktyk.

Warsztaty były również doskonałą okazją do dyskusji i wymiany doświadczeń z prekursorami programu o ochronie danych osobowych w codziennej pracy dydaktycznej. W ramach warsztatów zostały przedstawione propozycje interesujących zajęć i działań, które mogą być realizowane w szkołach i placówkach doskonalenia nauczycieli w ramach programu. Podczas szkolenia uczestnicy mogli również skorzystać z bezpłatnych konsultacji z ekspertami Biura GIODO i dowiedzieć się więcej, jak powinna wyglądać ochrona danych

osobowych w placówkach oświatowych. W szkoleniu udział wzięło ponad 150 przedstawicieli szkół i placówek doskonalenia nauczycieli, którzy przystąpili do V edycji programu.

8.2.7. Konferencje, seminaria, spotkania.

W roku sprawozdawczym 2014, 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 2014 r., Sympozja Świata Telekomunikacji i Mediów, czy Tydzień Zapobiegania Kradzieży Tożsamości oraz patronował takim przedsięwzięciom, jak konkurs wiedzy dla uczniów, czy wystawa „Dokumenty tożsamości", której organizatorem było Muzeum Warmii i Mazur. W 2014 r. Generalny Inspektor Ochrony Danych Osobowych objął swoim patronatem **51** wydarzeń zorganizowanych przez różne podmioty, których wykaz znajduje się w załączniku nr 6.

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. **Konferencja Naukowa „Przeszłość, teraźniejszość i przyszłość ochrony informacji niejawnych w zapewnianiu bezpieczeństwa narodowego RP" (Pułtusk, 22-23.01.2014 r.)**

Konferencja była okazją do przedstawienia prac nad ustawą o ochronie informacji niejawnych w związku z 15-leciem jej obowiązywania oraz do dyskusji i debaty eksperckiej na temat niedoskonałości obecnych przepisów i przyszłości regulacji prawnych dotyczących ochrony informacji niejawnych. Uczestnikiem tego wydarzenia był Pan Andrzej Lewiński – Zastępca Generalnego Inspektora Ochrony Danych Osobowych i zarazem członek Komitetu Honorowego Konferencji oraz prelegent, który omówił kwestie ochrony danych osobowych w przetwarzaniu informacji niejawnych.

2. **VIII Dzień Ochrony Danych Osobowych – 28 stycznia 2014 r.**

W dniu 28 stycznia 2014 r. Generalny Inspektor Ochrony Danych Osobowych już po raz ósmy organizował Europejski Dzień Ochrony Danych Osobowych ustanowiony przez

Komitet Ministrów Rady Europy. W tym dniu świętowana jest bowiem rocznica sporządzenia Konwencji Nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Konwencja ta jest najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych.

Uznając konieczność pogodzenia podstawowych wartości, takich jak poszanowanie prawa do prywatności i swobody przepływu informacji między ludźmi, Dzień Ochrony Danych Osobowych ustanowiony został dla podkreślenia odpowiedniej ochrony danych zarówno w życiu prywatnym, jak i zawodowym każdego obywatela. Zamiarem Rady Europy było ponadto uwrażliwienie obywateli na ochronę danych, a także poinformowanie o przysługujących im prawach oraz o dobrych praktykach. Dzień Ochrony Danych Osobowych ma zwrócić uwagę obywateli państw Europy na kwestie związane z ochroną danych osobowych i przyczynić się do podniesienia poziomu wiedzy w tym zakresie. W tym dniu, w całej Europie, odbywają się różnorodne spotkania, konferencje, warsztaty oraz inne imprezy towarzyszące, które są okazją do zdobycia wiedzy na temat ochrony danych, jak również umożliwiają wymianę poglądów między osobami zawodowo zajmującymi się tymi zagadnieniami.

Wydarzenia związane z VIII Dniem Ochrony Danych Osobowych odbywały się zarówno w Brukseli, jak i we wszystkich stolicach państw członkowskich Unii Europejskiej.

Z tej okazji Generalny Inspektor Ochrony Danych Osobowych zorganizował w Warszawie Dzień Otwarty, na który złożyła się konferencja, wykłady ekspertów, konferencja prasowa, 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. Tematem przewodnim ww. Ogólnopolskiej Konferencji zorganizowanej z okazji tego święta była „Prywatność w cyfrowym świecie", podczas której dyskutowano o podstawowych problemach wynikających z rozwoju nowoczesnych technologii i ich wpływie na życie społeczne i system prawny. Omawiane były w szczególności kwestie związane z aplikacjami mobilnymi, wyznaczania granic personalizacji w świecie BIG DATA, oraz wskazywano na konieczność powszechnej edukacji cyfrowej obywateli, jako warunku skutecznej ochrony prywatności.

Wśród gości wydarzeń zorganizowanych z okazji Dnia, znaleźli się przedstawiciele podmiotów sektora publicznego i gospodarczego, środowisk naukowych, organizacji pozarządowych, placówek oświatowych osób prywatnych oraz mediów.

Podmioty współpracujące z Generalnym Inspektorem Ochrony Danych Osobowych, jak szkoły czy ośrodki doskonalenia nauczycieli, również aktywnie włączyły się w obchody VIII Dnia Ochrony Danych Osobowych, organizując wydarzenia podkreślające wagę ochrony prywatności i danych osobowych. Natomiast Generalny Inspektor Ochrony Danych Osobowych był gospodarzem spotkania z uczniami jednej z warszawskich szkół gimnazjalnych z oddziałami integracyjnymi, podczas którego poprowadzone zostały zajęcia pt. „Świat wirtualny a rzeczywisty. Wyzwania i zagrożenia w Internecie. Czy czujesz się bezpieczny?".

Obchodom VIII Dnia Ochrony Danych Osobowych towarzyszyły również wydarzenia - za granicą. W Brukseli zaplanowano okolicznościowe spotkanie z europejskimi rzecznikami ochrony danych, a także wykład GIODO nt. reformy unijnych przepisów dotyczących ochrony danych osobowych, m.in. w kontekście programu PRISM, dla polskich europosłów.

3. Konferencja „Bezpieczeństwo w cyberprzestrzeni – czyli jak chronić tożsamość w Internecie" (Warszawa, 5.03.2014 r.)

Europejskie Stowarzyszenie Studentów Prawa ELSA Poland było organizatorem Konferencji, która z udziałem Generalnego Inspektora Ochrony Danych Osobowych odbywała się na Uniwersytecie Warszawskim. Podczas tego spotkania poszukiwano odpowiedzi na pytania dotyczące ochrony danych osobowych i bezpiecznego korzystania z sieci, cyberprzestępczości, dochodzenia swoich praw przed sądem, a także reformy unijnych przepisów dotyczących ochrony danych osobowych. Generalny Inspektor Ochrony Danych Osobowych był moderatorem jednego z paneli Konferencji.

4. II Konferencja „Safety and Security – Nowoczesne technologie, systemy i rozwiązania organizacyjne dla bezpieczeństwa informacji i danych osobowych" (Pułtusk, 19-21.03.2014 r.)

Celem Konferencji było omówienie i prezentacja najnowocześniejszych osiągnięć oraz innowacyjnych rozwiązań systemowych, organizacyjnych i technologicznych dotyczących bezpieczeństwa informacji i danych osobowych. Wśród nich znalazły się również zagadnienia dotyczące monitoringu wizyjnego, szpiegostwa gospodarczego, sprawowania nadzoru nad

dostępem do tajemnic prawnie chronionych i prowadzenia działań w zakresie zapobiegania, rozpoznawania, wykrywania i analizowania stanu potencjalnych zagrożeń. Uczestnikiem Konferencji był Pan Andrzej Lewiński, Zastępca GIODO, który przedstawił referat pt. „Prawne i praktyczne aspekty przetwarzania i transferu danych osobowych". Organizatorami Kongresu było Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego.

5. IV Konferencja Naukowa „Ataki sieciowe 2014" (Toruń, 24-25.03.2014 r.)

Celem Konferencji było zapoznanie uczestników z praktyką i metodologią związaną z przeprowadzaniem testów penetracyjnych i audytów bezpieczeństwa w przedsiębiorstwach, oraz prawne i praktyczne konsekwencje braku systemowego podejścia do bezpieczeństwa informacji w sieci. Podczas tego wydarzenia przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych wygłosił referat pt. „Zgłaszanie i klasyfikacja zgłoszeń naruszeń danych osobowych". Organizatorem spotkania było Studenckie Koło Naukowe Prawa Nowych Technologii działające na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, przy współpracy merytorycznej Centrum Badań nad Cyberprzestępczością.

6. Debata pt. „Ochrona danych osobowych a wybory" (Łódź, 26.03.2014 r.)

Centrum Ochrony Danych Osobowych i Zarządzania Informacją oraz Centrum Studiów Wyborczych, które działają na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, byli organizatorami debaty pt. „Ochrona danych osobowych a wybory", która z udziałem Generalnego Inspektora Ochrony Danych Osobowych odbyła się na Uniwersytecie Łódzkim. Podczas tego spotkania poruszane były m.in. tematy związane z obowiązkami administratorów danych przetwarzających dane wyborców w trakcie kampanii wyborczej, kto i na jakiej podstawie może zbierać dane osobowe wyborców i czy zbiory te podlegają obowiązkowi rejestracji GIODO.

7. VII Konferencja SEMAFOR (Warszawa, 27-28.03.2014 r.)

Bezpieczeństwu informacji, audytu, zarządzaniu ryzykiem oraz ochronie danych osobowych w przedsiębiorstwie poświęcona była kolejna, 7. edycja Konferencji SEMAFOR (Security, Management, Audit, Forum), która pod patronatem honorowym Generalnego Inspektora Ochrony Danych Osobowych odbywała się w dniach 27-28 marca 2014 r. w Warszawie. Podczas drugiego dnia Konferencji, Generalny Inspektor Ochrony Danych

Osobowych wygłosił referat pt. „Analityka predykcyjna jako teraźniejszość i przyszłość rynku przetwarzania danych. Spojrzenie rzecznika ochrony danych", w którym przybliżył zagadnienia związane z przewidywaniem współczesnych zagrożeń związanych z prawem do prywatności i ochrony danych osobowych w świetle szybkiego rozwoju nowoczesnych technologii. Organizatorami tego wydarzenia był magazyn Computerworld oraz stowarzyszenia ISSA Polska i ISACA Warsaw Chapter.

8. Konferencja „E-protokół a wymiar sprawiedliwości" (Warszawa, 31.03.2014 r.)

Stowarzyszenie Sędziów Polskich IUSTITIA było organizatorem Konferencji, podczas której rozważano, jak instytucja e-protokołu funkcjonuje w działalności sądów, w szczególności w kontekście efektywności toczących się postępowań. Omówiono również konsekwencje cyfryzacji czynności w postępowaniach przed sądem dla zasad ochrony danych osobowych i prywatności, w tym także psychologiczne aspekty nagrywania rozpraw. Podczas tego wydarzenia przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych przedstawił prezentację nt. „Jak zabezpieczyć dane osobowe w kontekście postępującej cyfryzacji sądów".

9. Debata pt. „Ochrona danych osobowych a wykonywanie zawodów prawniczych" (Łódź, 10.04.2014 r.)

Czy tajemnica zawodowa wyłącza konieczność stosowania przepisów ustawy o ochronie danych osobowych, kiedy należy stosować obowiązek informacyjny i czy wiąże on organy ochrony prawnej, kiedy przetwarzanie danych osobowych wymaga zawarcia umowy powierzenia danych, oraz jakie dokumenty o charakterze organizacyjnym powinny być opracowane w kancelarii, sądzie, urzędzie czy biurze rachunkowych – to tylko kilka przykładów zagadnień poruszanych podczas spotkania na Uniwersytecie Łódzkim. Debata odbywała się z udziałem przedstawicieli Generalnego Inspektora Ochrony Danych Osobowych, którzy przybliżyli słuchaczom zagadnienia związane z kompetencjami kontrolnymi GIODO i przebiegiem kontroli, w szczególności w kontekście zainteresowania przedstawicieli zawodów prawniczych zapowiadanym przez GIODO wzmożeniem kontroli w kancelariach prawnych. Organizatorem debaty było Centrum Ochrony Danych Osobowych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.

10. VI Forum Technologii Bankowości Spółdzielczej 2014 (Warszawa, 20-21.05.2014 r.)

Zagadnienia związane z nowymi rozwiązaniami produktowymi, technologicznymi i związanym z tym bezpieczeństwem usług banków spółdzielczych, a w szczególności innowacyjne rozwiązania teleinformatyczne w ofercie banków spółdzielczych, bankowość mobilna, usługi oferowane w chmurze a zagadnienia bezpieczeństwa informacji i danych osobowych, były głównym tematem dyskusji podczas tego spotkania. Przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych zapoznał uczestników Forum z tematem dotyczącym zasady celowości w procesie przetwarzania danych osobowych przez banki. Organizatorem tego wydarzenia było Centrum Prawa Bankowego i Informacji oraz Związek Banków Polskich.

11. Konferencja Naukowa „Jawność i tajność a sprawność administrowania" (Warszawa, 23 maja 2014 r.)

Jawność i tajność działania administracji publicznej była głównym tematem konferencji naukowej zorganizowanej na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. W ramach tego ogólnego tematu poruszane były zagadnienia dotyczące transparentności działania organów administracji publicznej i samorządowej, w szczególności traktowania „jawności" jako bariery sprawności działania administracji oraz wskazania formalnych podstaw odmowy dostępu do informacji publicznej. Podczas Konferencji Generalny Inspektor Ochrony Danych Osobowych wygłosił wykład pt. „Dokumentacja tworzona pod kątem udostępniania publicznego". Organizatorami tego wydarzenia, które odbywało się w ramach projektu badawczo-rozwojowego realizowanego na rzecz bezpieczeństwa i obronności Państwa pn. „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", byli: Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Minister Administracji i Cyfryzacji oraz Generalny Inspektor Ochrony Danych Osobowych.

12. Konferencja „Czego możemy oczekiwać po wirtualnych urzędach? Szanse i zagrożenia dla rozwoju e-administracji w Polsce" (Warszawa, 27.05.2014 r.)

Warunki przejrzystości działania sektora publicznego i dostęp do zasobów publicznych w sieci, a także rezultaty wprowadzenia e-usług publicznych i prezentacja najnowszych projektów informatyzacji polskiej administracji były głównymi tematami wystąpień podczas Konferencji. Uczestnicy spotkania rozmawiali również o korzyściach i zagrożeniach

związanych z cyfryzacją urzędów w naszym kraju. Przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych wystąpił w panelu poświęconym rozwojowi publicznych e-usług w Polsce, podczas którego dyskutowano o stanie upowszechnienia, możliwościach i ryzykach elektronicznych systemów usług w oparciu o wybrane przykłady. Organizatorem Konferencji było Koło Naukowe Administracji Publicznej (KNAP) działające na Wydziale Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego.

13. Konferencja pt. „Ochrona danych osobowych w działalności Kościołów i innych związków wyznaniowych" (Łódź, 30.05.2014 r.)

Przedmiotem tej Konferencji, zorganizowanej pod patronatem i we współpracy z Generalnym Inspektorem Ochrony Danych Osobowych na Uniwersytecie Łódzkim, była problematyka związana z przetwarzaniem danych osobowych członków Kościołów i innych wspólnot wyznaniowych. Wśród poruszonych zagadnień znalazła się m.in. kwestia konstytucyjnych uwarunkowań kognicji organów władzy publicznej w sprawach Kościołów i innych związków wyznaniowych, jako administratorów danych osobowych, a także kompetencje GIODO w odniesieniu do Kościołów w świetle ustawy o ochronie danych osobowych i orzecznictwa sądów administracyjnych. Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Przetwarzanie danych wiernych w systemach teleinformatycznych". Organizatorem Konferencji było Centrum Ochrony Danych Osobowych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.

14. Seminarium nt. biometrii (Warszawa, 17.09.2014 r.)

Organizatorem seminarium dotyczącego wykorzystania biometrii i innych nowoczesnych technologii w ochronie infrastruktury krytycznej, było Rządowe Centrum Bezpieczeństwa. Podczas tego spotkania omówione zostały zagadnienia związane z bezpiecznym wykorzystaniem biometrii i jej wdrożeniem w polskich dokumentach podróży, metodą oceny systemu biometrycznego oraz aspekt prawny procedur biometrycznych. Przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych przedstawił prezentację pt. „Prawna dopuszczalność przetwarzania danych osobowych w systemach biometrycznych", podczas której przybliżył operatorom infrastruktury krytycznej oraz przedstawicielom ministerstw i urzędów wojewódzkich zagadnienia związane z ochroną

danych osobowych w kontekście wykorzystywania biometrii w zarządzaniu kryzysowym elementami infrastruktury krytycznej.

15. III Konferencja Zarządzania Ciągłością Działania (Szczytno, 23-24.09.2014 r.)

„Zapewnienie Bezpieczeństwa i Ciągłości Funkcjonowania Organów Państwa w Obliczu Dzisiejszych Zagrożeń" było tematem III Konferencji Zarządzania Ciągłością Działania, która pod patronatem honorowym GIODO odbyła się w Wyższej Szkole Policji w Szczytnie. Rządowe Centrum Bezpieczeństwa objęło nad nią patronat merytoryczny. Celem tego spotkania była wymiana wiedzy i doświadczeń w zakresie szeroko rozumianego bezpieczeństwa państwa, obywateli i przedsiębiorców. Konferencja składała się z dwóch paneli dyskusyjnych: „Modele Ciągłości Działania i Zarządzania Ryzykiem a bezpieczeństwo państwa" i „Ryzyka związane z Ciągłością Działania, Korupcją i Bezpieczeństwem Informacji. Jak tworzyć bezpieczny łańcuch dostaw".

16. Międzynarodowa Konferencja „Lawyers in the Media Society (Łódź, 29.10.2014 r.)

Tematyka Konferencji odnosiła się do aktualnych problemów związanych z wpływem rozwoju nowoczesnych technologii informacyjnych na regulacje prawne w Unii Europejskiej, ze szczególnym uwzględnieniem prawa polskiego i fińskiego. Podczas tego wydarzenia Generalny Inspektor Ochrony Danych Osobowych przedstawił referat pt. „Law through the Lens of Information Retrival Systems. Most Common Lawyers'Mistakes" („Prawo przez pryzmat systemów wyszukiwania informacji. Najpoważniejsze błędy prawników"), w którym zaprezentował wieloaspektowe prawne spojrzenie na technologię informacyjną wykorzystywaną w pracy przedstawicieli zawodów prawniczych. Organizatorem tego wydarzenia była Katedra Europejskiego Prawa Gospodarczego Wydziału Prawa i Administracji Uniwersytetu Łódzkiego oraz Instytut Prawa i Informatyki Uniwersytetu Lapland.

17. IX doroczna Konferencja Zakładu Praw Człowieka WPiA UW (Warszawa, 14.11.2014 r.)

„Wpływ Europejskiej Konwencji Praw Człowieka na funkcjonowanie biznesu" – to tytuł dorocznej Konferencji Naukowej zorganizowanej przez Zakład Praw Człowieka Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, której 9. edycja w 2014 r. poświęcona została pamięci Profesora Jerzego Starościaka. Podczas tego wydarzenia

Generalny Inspektor Ochrony Danych Osobowych wystąpił w panelu poświęconym obowiązkom i uprawnieniom pracodawcy w kontekście praw jednostki zagwarantowanych w Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności. Tytuł wystąpienia GIODO brzmiał „Obowiązki pracodawcy w zakresie ochrony prawa do prywatności w świetle orzecznictwa ETPCz".

18. Seminarium pt. „Sędzia – osoba publiczna czy prawna? Granice dostępu do informacji publicznej i ochrony danych osobowych" (Łódź, 17.11.2014 r.)

W związku z wątpliwościami interpretacyjnymi dotyczącymi ochrony danych osobowych sędziów, zakresu udostępniania informacji o sędziach w ramach dostępu do informacji publicznej oraz granic ingerencji w prywatność osób pełniących funkcje publiczne, na Uniwersytecie Łódzkim odbyło się spotkanie osób zainteresowanych tą problematyką. Podczas tego wydarzenia przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych wygłosił referat pt. „Ograniczenia prawa do prywatności sędziego, jako osoby pełniącej funkcje publiczne". Organizatorami seminarium byli: Sąd Apelacyjny w Łodzi, Oddział Łódzki Stowarzyszenia Sędziów Polskich IUSTITIA oraz Centrum Ochrony Danych Osobowych i Zarządzania Informacją Wydziału Prawa i Administracji Uniwersytetu Łódzkiego.

19. Konferencja Naukowa „Prywatność i jawność: bilans 25-lecia" (Warszawa, 24.11.2014 r.)

Zagadnienia związane z prawem do prywatności, jawnością życia publicznego, a następnie wyważanie tych dwóch zasad prawnych w świetle najnowszego orzecznictwa sądów administracyjnych, w szczególności w kontekście możliwości współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych, to tylko niektóre tematy, które były przedmiotem obrad podczas tej Konferencji. Przedstawione też zostały kierunki zmian w regulacjach w zakresie dostępu do informacji publicznej, w szczególności w zakresie ponownego wykorzystania informacji sektora publicznego, a także dylematy związane z koncepcją skupienia w jednym organie kontroli ochrony danych osobowych i dostępu do informacji publicznej. Podczas tego wydarzenia Generalny Inspektor Ochrony Danych Osobowych wystąpił w panelu pod nazwą „Prywatność", w którym przedstawił referat dotyczący przyszłości prawa do prywatności oraz moderował debatę z udziałem przedstawicieli mediów, na temat granic jawności w działalności środków masowego

przekazu. Organizatorami Konferencji byli Dziekan Wydziału Prawa i Administracji Uniwersytetu Warszawskiego i Generalny Inspektor Ochrony Danych Osobowych we współpracy z Kołem Naukowym „CyberLaw" oraz Stowarzyszeniem Absolwentów Wydziału Prawa i Administracji UW. Patronat Honorowy nad tym wydarzeniem objął Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski, 25-lecie Wolności.

20. Konferencja „Security Case Study 2014" (Warszawa, 27.11.2014 r.)

Pod Patronatem Honorowym Generalnego Inspektora Ochrony Danych Osobowych odbywała się w Warszawie Konferencja „Security Case Study 2014", której organizatorem była Fundacja Bezpieczna Cyberprzestrzeń. Konferencja poświęcona była cyberbezpieczeństwu i popularyzacji wiedzy o zapobieganiu i walce z cyberzagrożeniami. W drugim dniu Konferencji odbyła się prezentacja aplikacji, które zwyciężyły w konkursie zorganizowanym przez Generalnego Inspektora Ochrony Danych Osobowych wspólnie z Ministerstwem Administracji i Cyfryzacji na aplikację mobilną przyjazną prywatności. Celem konkursu, któremu patronowała Fundacja Bezpieczna Cyberprzestrzeń, było zachęcenie młodych twórców aplikacji mobilnych do przestrzegania zasad ochrony danych osobowych. Prezentacja aplikacji przez zwycięskie zespoły zakończyła się uroczystością wręczenia nagród przez Generalnego Inspektora Ochrony Danych Osobowych.

21. Konferencja kończąca projekt PHAEDRA (Kraków, 12.12.2014 r.)

Międzynarodowa Konferencja „Egzekwowanie prywatności: wnioski z obecnego wdrażania i perspektywy na przyszłość" była ostatnim punktem projektu PHAEDRA (Improving Practical and Helpful co-operAtion between Data pRotection Authorities) realizowanego przez 4 instytucje: Vrije Universiteit Brussel (VUB-LSTS) z Belgii, Trilateral Research & Consulting LLP z Wielkiej Brytanii, Generalnego Inspektora Ochrony Danych Osobowych z Polski oraz Universitat Jaume I z Hiszpanii. Celem konferencji w Krakowie było zaprezentowanie rezultatów końcowych projektu i dyskusja na temat szerszej współpracy i koordynacji działań między organami ochrony danych osobowych, rzecznikami prywatności i organami wdrażania prawa prywatności. Ważnym punktem tego spotkania było omówienie barier prawnych i praktycznych w egzekwowaniu prawa do prywatności oraz właściwa identyfikacja ograniczeń (prawne i pozaprawne), na które napotykają organy ochrony danych w związku z wdrażaniem prawa do prywatności i ochrony danych osobowych, zarówno z punktu widzenia regulatorów, jak i interesariuszy (środowisko

naukowe, media). Konferencja skierowana była do organów ochrony danych osobowych, decydentów, przedstawicieli środowisk akademickich, organizacji pozarządowych oraz mediów.

22. VII Forum Nowej Gospodarki (Kraków, 15.12.2014 r.)

„Kierunek – Miasto Przyszłości" – to tytuł VII Forum Nowej Gospodarki, które zorganizowane zostało z inicjatywy Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie. Tematem przewodnim tego spotkania były gospodarcze i społeczne uwarunkowania powstawania w Polsce rozwiązań „inteligentnego miasta", w tym przełamywanie barier technologicznych, organizacyjnych i mentalnych związanych z realizacją projektów *smart city*, które obejmują zarówno codzienne życie miast, jak sytuacje nadzwyczajne. Uczestnikiem Forum był zastępca Generalnego Inspektora Ochrony Danych Osobowych, który przedstawił prezentację pt. „Inteligentne miasto a ochrona prywatności obywatela".

8.2.8. Porozumienia o współpracy

a) Społeczna Akademia Nauk z siedzibą w Łodzi, 25.02.2014 r.

„Porozumienie w sprawie współpracy pomiędzy GIODO a Społeczną Akademią Nauk", które zostało podpisane 25 lutego 2014 r. w Warszawie, dotyczy współpracy naukowo-badawczej, edukacyjnej, promocyjnej oraz wydawniczej w zakresie ochrony prywatności i danych osobowych, informacji niejawnych i innych tajemnic prawnie chronionych. Przewiduje m.in. wspólną organizację seminariów, konferencji, szkoleń i praktyk zawodowych oraz realizację prac naukowych i badawczych, m.in. z zakresu ochrony danych osobowych w systemach bezpieczeństwa państwa. Zakłada także wzajemne uczestnictwo pracowników GIODO i Społecznej Akademii Nauk w szkoleniach realizowanych w tych instytucjach.

b) Uniwersytet Jagielloński w Krakowie, 12.06.2014 r.

W dniu 12 czerwca 2014 r. w Krakowie zostało podpisane „Porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych" pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a Rektorem Uniwersytetu Jagiellońskiego. Współpraca realizowana będzie w obszarach działalności: naukowo-badawczej, edukacyjnej, promocyjnej i wydawniczej. Obie instytucje będą również wymieniać się materiałami o charakterze

analitycznym i informacyjnym, dokumentacją prawną oraz innymi danymi dotyczącymi form i metod pracy z zachowaniem tajemnic prawnie chronionych, a także organizować seminaria, konferencje, szkolenia, praktyki studenckie oraz wspólnie podejmować prace naukowe i badawcze z zakresu ochrony danych osobowych. Uniwersytet Jagielloński jest już 14. szkołą wyższą, z którą GIODO zawiera umowę mającą na celu zwiększenie wiedzy o prawach i środkach ochrony danych osobowych, poprzez m.in. wymianę doświadczeń i wzajemną pomoc.

c) Krajowa Agencja Ochrony Danych Osobowych Republiki Kosowa, 10.07.2014 r.

Podczas wizyty w Polsce delegacji Krajowej Agencji Ochrony Danych Osobowych Kosowa, w dniu 10 lipca 2014 r. w Warszawie, dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych oraz Ruzhdi Jashari, Główny Inspektor Krajowy Republiki Kosowa, podpisali „Porozumienie o współpracy między polskim i kosowskim organem ochrony danych osobowych". Celem Porozumienia jest potwierdzenie dalszego rozwoju stosunków miedzy GIODO a Krajową Agencją Ochrony Danych Osobowych Republiki Kosowa, jak również wzmocnienia ich roli w całym regionie (na poziomie Europy), w ramach gwarancji praw człowieka i wolności, w szczególności w zakresie ochrony danych osobowych.

8.2.9. Inne informacje

a) Powstanie Koalicji Infolinii

Infolinie i telefony pomocowe stanowią dla obywateli jedno z ważniejszych źródeł zdobywania informacji. Stąd z inicjatywy Rzecznika Praw Obywatelskich i Fundacji „Dzieci Niczyje" powstała grupa telefonicznego wsparcia obywateli – Koalicja Infolinii, w skład której weszła również Infolinia GIODO. Celem działania Koalicji jest wymiana doświadczeń, organizacja wspólnych szkoleń i podnoszenie poziomu udzielanej pomocy poprzez wypracowanie jednolitych standardów w zakresie poradnictwa telefonicznego. Spotkanie inauguracyjne Koalicji Infolinii odbyło się 13 czerwca 2014 r. w Biurze Rzecznika Praw Obywatelskich. Uczestniczyli w nim przedstawiciele 14 Infolinii i telefonów pomocowych, wśród których obecna była dyrektor Zespołu Rzecznika Prasowego, odpowiedzialnego za funkcjonowanie Infolinii w Biurze GIODO. W 2014 r. odbyły się trzy szkolenia dla przedstawicieli Infolinii i telefonów pomocowych z udziałem przedstawiciela GIODO obsługującego Infolinię. Ich organizatorami byli kolejno: Rzecznik Praw Obywatelskich,

Rzecznik Praw Pacjenta oraz Fundacja „Dzieci Niczyje". Podczas warsztatów omawiane były konkretne kazusy przygotowane przez pracowników obsługujących Infolinię i przyjęcia interesantów w siedzibie danego organizatora szkolenia. Natomiast dodatkowym atutem szkolenia zorganizowanego przez Fundację „Dzieci Niczyje" było rozwijanie wśród uczestników praktycznych umiejętności świadczenia pomocy telefonicznej osobom będącym w kryzysie emocjonalnym. Celem tego szkolenia było m.in. skuteczne przekazywanie informacji o ofercie Infolinii lub telefonu pomocowego, zachęcanie do podjęcia określonych działań, w tym wskazywanie właściwych instytucji. W listopadzie 2014 r. z inicjatywy Rzecznika Praw Obywatelskich ukazał się informator o telefonach pomocowych prowadzonych przez instytucje publiczne i organizacje pozarządowe, w celu ułatwienia osobom poszukującym informacji w dotarciu do odpowiedniego adresata. W publikacji tej, wśród wymienionych instytucji, znajduje się również informacja na temat Infolinii działającej w Biurze Generalnego Inspektora Ochrony Danych Osobowych. Informacja o Informatorze Telefonów Pomocowych została zamieszczona na stronie internetowej GIODO.

b) Spotkanie GIODO ze studentami kół naukowych

W dniu 23 maja 2014 r. w siedzibie Generalnego Inspektora Ochrony Danych Osobowych w Warszawie, odbyło się spotkanie studentów z Koła Naukowego Prawa Nowych Technologii działającego na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, a także studentów z kół naukowych z Uniwersytetu w Katowicach, Białymstoku i Poznaniu.

Spotkanie było odpowiedzią na wzrost zainteresowania studentów zagadnieniami przetwarzania danych osobowych, w szczególności unijną reformą przepisów o ochronie danych. Spotkanie było jednocześnie okazją do przedyskutowania kwestii związanych z uprawnieniami kontrolnymi Generalnego Inspektora Ochrony Danych Osobowych oraz jego doświadczeniami w tym zakresie, karami za łamanie przepisów ustawy o ochronie danych osobowych, a także aplikacjami mobilnymi a ochroną danych osobowych oraz oceną rozwiązań prawnych w tym zakresie. Te oraz inne zagadnienia, przybliżył przybyłym gościom Generalny Inspektor Ochrony Danych Osobowych oraz przedstawiciele jego Biura.

c) GIODO członkiem Forum Strategicznego Centrum Zaawansowanych Technologii Miasta Przyszłości

W 2014 r. Generalny Inspektor Ochrony Danych Osobowych został członkiem Forum Strategicznego Centrum Zaawansowanych Technologii Miasta Przyszłości – CZTMP, działającego przy Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie. Podstawowym celem Forum jest wypracowanie polskiego modelu inteligentnego miasta i opracowanie wynikających z niego rekomendacji dla środowisk naukowych, biznesu i samorządu terytorialnego. Zadaniem CZTMP jest integracja i koordynacja aktywności i działań służących wypracowywaniu i rozpowszechnianiu innowacyjnych rozwiązań opartych m.in. na zintegrowanych technologiach informacyjno-komunikacyjnych.

9. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Jednym z ustawowych 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, udział w pracach Komitetu Konsultacyjnego Rady Europy, 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, oraz udział w organizowanych cyklicznie Międzynarodowych Konferencjach Rzeczników Ochrony Danych i Prywatności, Wiosennych Konferencjach Europejskich Organów Ochrony Danych oraz w Warsztatach Rozpatrywania Spraw. 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, wspólnego organu nadzorczego Europolu, a także Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji (tzw. Grupa Berlińska).

9.1. Komitet Konsultacyjny do spraw Konwencji Nr 108 (T-PD).

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 roku 2014 r. 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. Modernizacja tego najstarszego, ponad trzydziestoletniego aktu prawa dotyczącego ochrony danych, wynikała z konieczności sprostania współczesnym wyzwaniom wynikającym z powszechnego stosowania nowoczesnych technologii informacyjnych i komunikacyjnych oraz wzmocnienia efektywnego wdrażania jej postanowień. Podczas 31. Posiedzenia T-PD, które odbyło się w dniach 2-4 czerwca 2014 r., członkowie Komitetu zajmowali się kwestiami dotyczącymi modernizacji Konwencji. Ponadto zakończono prace nad projektem zrewidowanej rekomendacji w sprawie ochrony danych osobowych wykorzystywanych do celów zatrudnienia. Dokument ten został przekazany do Komitetu Ministrów Rady Europy celem przyjęcia. Wśród szeregu innych kwestii, które zostały poruszone na tym spotkaniu, znalazły się m.in. ochrona danych w pracy policji, rekomendacja w sprawie danych medycznych, Big Data, współpraca z organami Rady Europy, projekt opinii – wpływ mechanizmów automatycznej międzypaństwowej wymiany danych osobowych do celów administracyjnych i podatkowych na ochronę danych, projekt opinii – Rekomendacja PACE 2041 (2014) – „Poprawa ochrony i bezpieczeństwa użytkownika w cyberprzestrzeni".

9.2. Grupa Robocza Art. 29.

W omawianym roku sprawozdawczym 2014, 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[465] 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 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[466].

Na uwagę zasługuje, że podczas 94 posiedzenia Grupy Roboczej, pierwszego w 2014 r., które odbywało się w dniach 26-27 lutego 2014 r., wybrano na dwuletnią kadencję nowe władze tego niezależnego europejskiego organu doradczego Komisji Europejskiej do spraw ochrony danych osobowych i prywatności. Na stanowisko Przewodniczącego Grupy Roboczej Art. 29 powołano przewodniczącą francuskiego organu ochrony danych (CNIL) – Isabelle Falque-Pierrotin. Wiceprzewodniczącymi zostali dr Wojciech R. Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, oraz Gérard Lommel, Przewodniczący luksemburskiego organu ochrony danych.

Istotne znaczenie dla unijnej ochrony danych w odniesieniu do wyszukiwarek ma wyrok Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 13 maja 2014 r. w sprawie Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja Gonzáles (C-131/12). Przyznaje on osobom, których dane dotyczą, możliwość składania do operatorów wyszukiwarek, pod określonymi warunkami, wniosków o usunięcie linków do informacji ich dotyczących, pojawiających się w wynikach wyszukiwania w rezultacie wyszukiwania przeprowadzonego na podstawie nazwiska osoby. Nie wymaga to usuwania linku z indeksów wyszukiwarki całkowicie. Oznacza to, że oryginalne informacje nadal będą dostępne po użyciu innych terminów wyszukiwania lub poprzez bezpośredni dostęp do źródła. W dniu 25 listopada 2014 r. europejskie organy ochrony danych zrzeszone w ramach Grupy Roboczej Artykułu 29 przyjęły **wytyczne w**

[465] Art. 30 ust. 1 dyrektywy 95/46/WE.
[466] Art. 15 ust. 3 dyrektywy 2002/58/WE.

sprawie implementacji ww. wyroku. Dokument ten zawiera ich wspólną interpretację tego wyroku oraz określa jednakowe kryteria do stosowania przez organy ochrony danych podczas rozpatrywania skarg na operatorów wyszukiwarek. Podkreślenia wymaga, że żadne z pojedynczych kryteriów nie ma samo w sobie charakteru decydującego. Każde z kryteriów należy odczytywać w świetle zasad ustalonych przez Trybunał, a w szczególności w świetle interesu opinii publicznej w zakresie uzyskania dostępu do informacji.

9.3. Inne.

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 dniu 20 marca 2014 r. Było to już czwarte 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 2014 r. przedstawiciel GIODO uczestniczył również w posiedzeniach Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupy Berlińskiej)[467], z których jedno odbyło się w dniach 5-6 maja 2014 r. w Skopje, drugie zaś 14-15 października 2014 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. W szczególności przedstawiony został stan prac nad ustawą regulującą zasady funkcjonowania monitoringu wizyjnego, do projektu której GIODO zgłosił szereg uwag. Wśród nich znalazły się m.in. zastrzeżenia dotyczące braku ograniczenia stosowania monitoringu w miejscu pracy oraz braku wymagań przeprowadzenia

[467] International Working Group on Data Protection in Telekomunications – IWGDPT.

analizy wpływu na prywatność dla systemów wyposażonych w elementy automatycznego rozpoznawania obiektów i ich zachowań. Ponadto w 2014 r. do Biura GIODO wpłynęły też skargi dotyczące trudności w wyegzekwowaniu od Google realizacji wniosków o usunięcie linków do informacji naruszających prywatność konkretnych osób. Skarżący informowali GIODO o braku reakcji na zgłoszone za pośrednictwem strony internetowej wnioski, jak również o braku odpowiedzi na ponaglenia kierowane w tych sprawach do siedziby Google w Polsce.

9.3.1. Agencja Praw Podstawowych.

Od 2007 r. Generalny Inspektor Ochrony Danych Osobowych współpracuje z **Agencją Praw Podstawowych Unii Europejskiej – APP (The European Union Agency for Fundamental Rights – FRA)** – unijnym organem zajmującym się monitorowaniem przestrzegania praw obywatelskich w Unii Europejskiej. APP co roku przeprowadza konsultacje z państwami członkowskimi i organizacjami społecznymi w celu uzgodnienia rocznego programu prac Agencji na kolejny rok kalendarzowy. Za pomocą kwestionariusza APP zapoznaje się z opiniami swoich partnerów o planowanych przez nich na kolejny rok działaniach. Konsultacja ma na celu zbadanie, czy wskazane w kwestionariuszu dziedziny aktywności i bloki tematyczne zostały poprawnie zidentyfikowane przez Agencję oraz czy należą one do priorytetowych obszarów zainteresowania państw członkowskich.

W dniu 28 stycznia 2014 r. opublikowany został podręcznik dotyczący europejskiego prawa ochrony danych (Handbook on European data protection law), opracowany wspólnie przez Agencję Praw Podstawowych Unii Europejskiej oraz przez Radę Europy wraz z Kancelarią Europejskiego Trybunału Praw Człowieka. Jest to trzeci z serii podręczników prawniczych przygotowany wspólnie przez Agencję Praw Podstawowych i Radę Europy. Publikacja ta ma na celu podniesienie świadomości i wiedzy na temat przepisów w zakresie ochrony danych w państwach członkowskich Unii Europejskiej i Rady Europy, służąc jako główny punkt odniesienia dla czytelników. Przeznaczony jest dla prawników nie specjalizujących się w tej dziedzinie, sędziów, krajowych organów ochrony danych oraz innych osób pracujących w dziedzinie ochrony danych. Obecnie Podręcznik dostępny jest w wersji angielskojęzycznej, ale będzie przetłumaczony również na język polski. Agencja Praw Podstawowych konsultowała z GIODO polską terminologię terminów prawniczych z zakresu ochrony danych osobowych, wykorzystanych w publikacji.

Generalny Inspektor Ochrony Danych Osobowych był również zaangażowany w prace nad raportem „Dostęp do środków odwoławczych w zakresie ochrony danych w państwach członkowskich UE" („Access to data protection remedies in EU Member Status") oraz „Opracowaniem APP dotyczącym elementów niezależności organów ochrony danych w UE" („FRA draft study on elements of independence of the data Protection authorities in the EU"). GIODO wniósł wkład do kwestionariusza będącego podstawą Opracowania oraz przedstawił uwagi do tego projektu przed jego publikacją.

9.3.2. GPEN.

Na uwagę zasługuje aktywny udział Generalnego Inspektora Ochrony Danych Osobowych w Corocznej Konferencji International Enforcement Coordination Annual Event, poświęconej koordynacji międzynarodowego egzekwowania prawa. Celem spotkania było zaprezentowanie dotychczasowej działalności **Światowej Sieci Egzekwowania Przepisów o Ochronie Prywatności (Global Privacy Enforcement Network – GPEN)** - której GIODO jest członkiem od listopada 2010 r.[468] - intensyfikacja współpracy, w tym możliwość przyjęcia nowych członków. Kanada i Zjednoczone Królestwo, gospodarze tego spotkania, przedstawili projekt **Transgranicznego porozumienia w sprawie współpracy przy egzekwowaniu prawa.** Uczestnicy spotkania w większości wyrazili uznanie dla tej propozycji, niemniej jednak uznali za konieczne przeprowadzenie konsultacji prawnych, w jaki sposób poszczególne organy mogłyby przystąpić do tego porozumienia oraz wskazały na konieczność uzupełnienia tego dokumentu o przepisy dotyczące zasad poufności obowiązujących w poszczególnych krajach, przestrzeganie zasady wzajemności, tj. udzielanie odpowiedzi w każdej sytuacji, nawet jeśli w odpowiedzi znajdzie się wskazanie, że dany rzecznik ochrony danych (Data Protection Authority – DPA) nie ma możliwości ani środków lub po prostu nie jest zainteresowany tematem. Ponadto w dokumencie powinny zostać określone kody wiarygodności danych, realistyczne ramy czasowe, w jakich DPA powinny udzielić odpowiedzi na pytanie, definicja *informacji poufnej*, a także sankcje za nieprzestrzeganie porozumienia.

Organizatorem tego wydarzenia był Urząd Rzecznika Informacji w Wilmslow i Styal w Zjednoczonym Królestwie (Information Commissioner's Office – ICO). Kolejne spotkania zaplanowane zostały w 2015 r. w Ottawie (Kanada) oraz w 2016 r. w Krakowie.

[468] http://www.giodo.gov.pl/591/id_art/3938/j/pl/

9.4. 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.

Pierwszym w kolejności międzynarodowym wydarzeniem 2014 roku, współorganizowanym przez GIODO, były uroczystości związane z obchodami **VIII Europejskiego Dnia Ochrony Danych Osobowych, które odbywały się w Brukseli w dniach 20-22 stycznia 2014 r.** W trakcie obchodów tego święta Generalny Inspektor Ochrony Danych Osobowych wziął udział w sesji polskiej podczas 7. Międzynarodowej Konferencji pt. „Computers, Privacy and Data Protection (CPDP) 2014. Reforming Data Protection: the Global Perspective", podczas której oprócz zagadnień związanych z pracami nad reformą ochrony danych w UE, omawiane były m.in. tematy dotyczące BIG DATA i dostępowi władz publicznych do informacji o obywatelach (w szczególności w kwestii gromadzenia danych dotyczących mniejszości), a także cyberprzestępczości, biometrii, e-zdrowia, cloud computingu oraz egzekwowania prawa przez organy ochrony danych osobowych. Pod patronatem tej Konferencji odbyło się również spotkanie partnerów projektu PHAEDRA z przedstawicielami europejskich organów ochrony danych i rzeczników prywatności oraz instytucji zajmujących się ochroną prywatności na poziomie ogólnoświatowym. Ponadto Generalny Inspektor ochrony Danych Osobowych zorganizował - w siedzibie Stałego Przedstawicielstwa RP przy UE w Brukseli uroczyste spotkanie 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.

Wśród najważniejszych wydarzeń o charakterze międzynarodowym, które odbyły się z udziałem GIODO lub jego przedstawicieli znalazły się:

1. **7. Międzynarodowa Konferencja „Computers, Privacy and Data Protection (CPDP) 2014" (Bruksela, 22-24.01.2014 r.)**

W związku z obchodami Europejskiego Dnia Ochrony Danych Osobowych, tradycyjnie od 7 lat odbywa się w Brukseli Międzynarodowa Konferencja „Komputery, Ochrona Danych

i Prywatności". Współorganizowali ją partnerzy z Europy i Azji. CPDP 2014 poświęcona była problematyce ważnej dla krajów reprezentujących region Ameryki Łacińskiej i Azji – Pacyfiku oraz Indii. W trakcie 60 paneli dyskutowano m.in. o reformie unijnych regulacji o ochronie danych, Big Data, cyberprzestępczości, przechowywaniu danych, przetwarzaniu w chmurze, egzekwowaniu prawa, biometrii, e-Zdrowiu, prywatności na etapie projektowania (*privacy by design*) oraz o zagadnieniach etycznych związanych ze zbieraniem danych mniejszości narodowych i wykorzystywaniem nowoczesnych technologii. Generalny Inspektor Ochrony Danych Osobowych uczestniczył w panelu poświęconym reformie unijnych przepisów o ochronie danych. Panelistami Konferencji byli przedstawiciele Komisji Europejskiej, Parlamentu Europejskiego, Europejskiego Rzecznika Ochrony Danych, Rady Europy oraz wielu innych organizacji, w tym studenckich. Konferencji towarzyszyło PechaKucha oraz inne publiczne debaty prowadzone w języku angielskim i niderlandzkim. Konferencja CPDP jest platformą non-profit założoną w 2007 r. przez grupę naukowców reprezentujących Vrije Universiteit Brussel, Université de Namur oraz Tilburg University. W chwili obecnej Konferencję CPDP tworzy konsorcjum 21 partnerów.

2. Warsztaty Komisji Europejskiej nt. cywilnych zastosowań zdalnie sterowanych systemów lotniczych (RPAS) (Bruksela, 28.02.2014 r.)

Celem spotkania europejskich organów ochrony danych było omówienie kwestii ochrony danych osobowych i prywatności w kontekście cywilnych zastosowań zdalnie sterowanych systemów lotniczych (RPAS), tzw. dronów. Przedstawione zostały informacje nt. obecnej i planowanej ewolucji uregulowań dotyczących bezpieczeństwa RPAS oraz przegląd rynku. Ponadto omówiono zagadnienie wspierania przez KE przyszłych inicjatyw GR Art. 29 lub krajowych organów ochrony danych. Organizatorem tego nieformalnego spotkania była Dyrekcja Generalna ds. Przedsiębiorstw i Przemysłu.

3. High Level Conference on the EU Cybersecurity Strategy (Bruksela, 28.02.2014 r.)

Konferencja wysokiego szczebla poświęcona strategii UE w zakresie cyberbezpieczeństwa. Konferencja miała na celu podsumowanie rocznego okresu, jaki upłynął od przyjęcia ww. strategii. Przedstawiono informacje nt. wdrożenia pięciu priorytetowych elementów tej strategii oraz głównych działań podjętych w jej ramach. Konferencja była również okazją do zastanowienia się nad kierunkami dalszych działań w związku z wnioskiem Komisji dotyczącym dyrektywy określającej środki służące

zapewnieniu wysokiego poziomu bezpieczeństwa sieci i informacji w całej UE oraz podjęciem kroków w celu wzmocnienia zaufania w sektorze publicznym i prywatnym na rzecz obywateli i Jednolitego Rynku Cyfrowego. Organizatorem tego wydarzenia była Komisja Europejska we współpracy z Europejską Służbą Działań Zewnętrznych.

4. Okrągły Stół OECD (Paryż, 21.03.2014 r.)

W dniu 21 marca 2014 r. przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych uczestniczył w obradach eksperckich Okrągłego Stołu OECD, pt. „Ochrona prywatności w gospodarce napędzanej danymi: ocena obecnego myślenia". Wśród uczestników obrad znaleźli się eksperci oraz delegaci z Grupy Roboczej OECD ds. Bezpieczeństwa i Ochrony Prywatności w Gospodarce Cyfrowej.

5. Warsztaty poświęcone zagrożeniom prywatności (Paryż, 20 marca 2014 r.)

Warsztaty zorganizowane zostały w związku z projektem ram dotyczących zagrożeń ochrony prywatności przez Centre for Information Policy Leadership (CPLI) w Paryżu. Projekt ten jest kontynuacją pionierskich prac prowadzonych przez Centrum nt. odpowiedzialności i rozliczalności za naruszenia prywatności, w szczególności koncepcji podejścia opartego na ryzyku w dziedzinie prawa i jego stosowania. Przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych wystąpił w nich jako mówca podczas sesji pt. „Jak ustawodawcy regulujący zagadnienia ochrony prywatności uwzględniają zagrożenia ochrony prywatności w pracach nad egzekwowaniem prawa?". Uczestniczył ponadto w obradach Okrągłego Stołu ekspertów OECD, poświęconych Big Data oraz analityce.

6. XVI Spotkanie Rzeczników Ochrony Prywatności z Krajów Europy Środkowej i Wschodniej (Skopje, 1-3.04.2014 r.)

W dniach 1-3 kwietnia 2014 r. w Skopje przedstawiciele Generalnego Inspektora Ochrony Danych Osobowych wzięli udział w 16 Spotkaniu Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA)[469]. Gospodarzem tegorocznego wydarzenia był organ ochrony danych Republiki Macedonii. Wśród uczestników spotkania znaleźli się przedstawiciele 14 organów ochrony danych

[469] 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.

z następujących krajów: Albanii, Bułgarii, Republiki Czeskiej, Czarnogóry, Macedonii, Węgier, Serbii, Polski, Rumunii, Słowacji, Słowenii, Bośni i Hercegowiny, Gruzji, Mołdawii, oraz przedstawiciele Rady UE. W trakcie Spotkania przyjęto Deklarację w sprawie nowego członka Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, na mocy której w poczet członków Grupy przyjęto organ ochrony danych z Gruzji, oraz Deklarację w sprawie wzajemnej pomocy i wzmocnionej współpracy. Druga Deklaracja miała na celu wyrażenie wspólnej potrzeby wzmocnienia współpracy oraz zwrócenie uwagi na obecny stan prac nad zmianą ram prawnych ochrony danych UE.

Została podjęta również decyzja, że 17. spotkanie CEEDPA odbędzie się w 2015 r. w Albanii, zaś 18. zostanie zorganizowane w 2016 r. w Bośni i Hercegowinie.

7. Warsztaty poświęcone certyfikatom z zakresu ochrony prywatności (Bruksela, 8 kwietnia 2014 r.)

GIODO oraz jego przedstawiciel brali udział w warsztatach poświęconych certyfikatom ochrony prywatności w Brukseli, organizowanych przez Wspólnotowe Centrum Badawcze Komisji Europejskiej, Instytut Ochrony i Bezpieczeństwa Obywateli (IPSC) oraz Dyrekcję Generalną ds. Sprawiedliwości, Trilateral Research & Consulting (wraz z partnerami projektu Vrije Universiteit Brussel i Intrasoft International SA). Warsztaty zorganizowane zostały w związku z badaniem w zakresie certyfikatów ochrony prywatności UE realizowanym przez Trilateral na rzecz Komisji Europejskiej w celu zebrania opinii na temat możliwości wprowadzenia ogólnoeuropejskiej certyfikacji ochrony prywatności, w myśl artykułu 39 projektu ogólnej dyrektywy o ochronie danych.

8. Konferencja pt. „Zbiory danych, informowanie obywateli: paszport do ochrony danych osobowych" (Bruksela, 9 kwietnia 2014 r.)

Generalny Inspektor Ochrony Danych Osobowych wziął udział w Otwartej Konferencji pt. „Zbiory danych, informowanie obywateli: paszport do ochrony danych osobowych", zorganizowanej przez Europejskie Stowarzyszenie Ochrony Praw Człowieka (AEDH), francuską Ligę Praw Człowieka (LDH), węgierskie stowarzyszenie Unia Praw Obywatelskich, niemieckie stowarzyszenie Humanistische Union, luksemburską Ligę Praw Człowieka (ALOS-LDH) oraz Europejskie Stowarzyszenie Sędziów i Prokuratorów na rzecz Demokracji i Wolności (MEDEL - European Magistrates for Democracy and Freedom) w siedzibie Europejskiego Komitetu Ekonomiczno-Społecznego w Brukseli. Podczas tego

wydarzenia Generalny Inspektor wygłosił referat pt. „Organy ochrony danych i organy nadzorcze: możliwości skutecznej ochrony danych osobowych obywateli?".

9. Międzynarodowa Konferencja „Data Protection Intensive" (Londyn, 29.04.-01.05.2014 r.)

W trakcie Międzynarodowej Konferencji „Data Protection Intensive" w Londynie dyskutowano o nowym prawie ochrony danych w Unii Europejskiej, usługach mobilnych, Big Data czy prywatności w Internecie. Generalny Inspektor Ochrony Danych Osobowych wziął udział w sesji eksperckiej poświęconej przyszłości uprawnień wykonawczych organów ochrony danych w Europie, podczas której porównywano uprawnienia wykonawcze dotyczące ochrony danych w krajach członkowskich UE w odniesieniu do zmian zaproponowanych w tym obszarze w projekcie ogólnego unijnego rozporządzenia o ochronie danych. Organizatorem tego międzynarodowego wydarzenia było IAPP (International Association of Privacy Professionals) zrzeszające praktyków z 83 krajów zajmujących się tematyką ochrony prywatności.

10. 2. Warsztaty projektu PHAEDRA (Skopje, 6 maja 2014 r.)

Organ Ochrony Danych Republiki Macedonii, który był gospodarzem spotkania Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji (International Working Group on Data Protection In Telecommunications – IWGDPT), zwanej Grupą Berlińską, zorganizował w jego ramach 2. warsztaty uczestników projektu PHAEDRA, pn. „Wyzwania i bariery współpracy i koordynacji działań pomiędzy organami ochrony danych osobowych". Warsztaty te przebiegały w formule okrągłego stołu. Członkowie konsorcjum przedstawili dotychczasowe rezultaty projektu, a następnie wspólnie z przedstawicielami organów ochrony danych debatowali nad określeniem barier międzynarodowej współpracy i koordynacji pomiędzy krajowymi organami ochrony danych osobowych (DPAs), rzecznikami ds. ochrony prywatności (PCs) oraz organami ds. egzekwowania ochrony danych osobowych i prywatności (PEAs) oraz wspólnie szukali skutecznego sposobu ich eliminowania.

11. Wiosenna Konferencja Rzeczników Ochrony Danych (Strasburg, 6.06.2014 r.)

Generalny Inspektor Ochrony Danych Osobowych oraz Dyrektor Departamentu Edukacji Społecznej Współpracy Międzynarodowej wzięli udział w zorganizowanej przez

Radę Europy oraz francuski organ ochrony danych (CNIL) Wiosennej Konferencji Europejskich Organów Ochrony Danych pt. „Współpraca europejska i międzynarodowa w obszarze ochrony danych". Podczas sesji poświęconej współpracy europejskiej i międzynarodowej dr Wojciech R. Wiewiórowski, GIODO, wygłosił wystąpienie pt. „Współpraca w obszarze najlepszych praktyk". W trakcie Konferencji Europejscy Rzecznicy Ochrony Danych przyjęli dwie rezolucje: „Rezolucję w sprawie akredytacji, na mocy której organ ochrony danych Gruzji został akredytowany jako członek Konferencji Europejskich Organów Ochrony Danych" oraz „Rezolucję w sprawie rewizji Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja 108)".

12. 3. Warsztaty projektu PHAEDRA (Seul, 18 czerwca 2014 r.)

Komisja Ochrony Prywatności Informacji (Personal Information Protection Commission – PIPC), południowokoreański organ ochrony danych osobowych, była gospodarzem 41. Asia Pacific Privacy Authorities Forum – APPA, które odbywało się w dniach 17-18 czerwca 2014 r. w Seulu. Podczas otwartej sesji drugiego dnia tego spotkania odbyły się 3. warsztaty projektu PHAEDRA, pn. „Rozporządzenie UE o ochronie danych osobowych w perspektywie udoskonalenia współpracy na poziomie regionalnym pomiędzy organami ochrony danych osobowych (DPAs), rzecznikami ds. ochrony prywatności (PCs) oraz organami ds. egzekwowania ochrony danych osobowych i prywatności (PEAs)". Generalny Inspektor Ochrony Danych Osobowych przedstawił założenia unijnej reformy ochrony danych osobowych oraz dotychczasowe wyniki projektu PHAEDRA. Natomiast dwaj mówcy spoza Europy przedstawili punkty widzenia na ten temat widziane z perspektywy swoich regionów, skupiając się na obecnych praktykach dotyczących współpracy międzyregionalnej i międzynarodowej pomiędzy DPAs, PCs i PEAs. Prezentacje te w szczególności odnosiły się do zidentyfikowanych barier prawnych, kulturowych, organizacyjnych, technicznych i innych oraz stojących przed nimi wyzwań, w perspektywie możliwości przyjęcia nowego rozporządzenia UE o ochronie danych.

13. Warsztaty podsumowujące projekt partnerski Leonardo da Vinci (Gdańsk, 25 czerwca 2014 r.)

W dniu 25 czerwca 2014 r. w Gdańsku, podczas organizowanych w Trójmieście IV Dni Otwartych GIODO, odbyły się warsztaty podsumowujące projektu partnerskiego Leonardo - da Vinci *„Zwiększanie świadomości w zakresie ochrony danych osobowych wśród*

pracowników zatrudnionych w krajach Unii Europejskiej", finansowanego przez Komisję Europejską w ramach programu „Uczenie się przez całe życie". Podczas tego spotkania Generalny Inspektor Ochrony Danych Osobowych przedstawił prezentację pt. „Internet of Things as a Challenge for the Privacy Protection in the Workplace". Ważną częścią warsztatów była oficjalna prezentacja publikacji pt. „Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników", której współautorami były organy ochrony danych z Polski, Czech, Bułgarii i Chorwacji.

14. Warsztaty rozpatrywania spraw (Skopje, 6-7 października 2014 r.)

Pracownicy Biura Generalnego Inspektora Ochrony Danych Osobowych systematycznie uczestniczą w warsztatach rozpatrywania spraw z zakresu ochrony danych osobowych, tzw. warsztatach skargowych (case handling workshop). Warsztaty te odbywają się z udziałem przedstawicieli organów ochrony danych osobowych działających zarówno na poziomie krajowym jak i lokalnym oraz Europejskiego Inspektora Ochrony Danych. Celem tych spotkań jest wymiana doświadczeń pomiędzy pracownikami poszczególnych organów, którzy na co dzień zajmują się rozpatrywaniem skarg lub przeprowadzaniem inspekcji. W dniach 6-7 października 2014 r. w Skopje odbyły się 26. warsztaty rozpatrywania spraw, zorganizowane przez Dyrekcję Organów Ochrony Danych Osobowych Republiki Macedonii - z udziałem 66 przedstawicieli organów ochrony danych oraz EIODO. Poszczególne sesje tematyczne dotyczyły tematów związanych z ochroną danych osobowych w działalności sądów oraz banków i innych instytucji finansowych, a także z wideonadzorem, biometrią, marketingiem, przekazywaniem danych osobowych krajom trzecim i organizacjom międzynarodowym przez instytucje i organy UE, a także zagadnień związanych z zachowaniem równowagi pomiędzy prawem dostępu obywateli do informacji publicznej a ochroną danych osobowych. Podczas tych warsztatów przedstawiciel GIODO przedstawił prezentację na temat „Prawo do prywatności w sieci a udostępnianie danych na potrzeby postępowania sądowego – prawo do sądu"[470].

15. 36. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności (Mauritius, 13-16.10.2014 r.)

[470] Materiały z 26. warsztatów rozpatrywania spraw można znaleźć na stronie internetowej organizatora, w zakładce „26th case handling workshop" - http://www.privacy.mk/sq/CHW_Presentations.

Rozwój nowoczesnych technologii, postępująca globalizacja i stopień komplikacji kwestii związanych z wykorzystywaniem danych osobowych powodują, że rzecznicy ochrony danych osobowych z kilkudziesięciu krajów świata, na czele z Europejskim Inspektorem Ochrony Danych, a także przedstawiciele instytucji UE, rządów państw, eksperci zajmujący się tą problematyką, przedstawiciele biznesu i świata akademickiego, organizacje pozarządowe i międzynarodowe działające na rzecz praw człowieka, spotykają się regularnie od 36 lat, by wspólnie dyskutować o najważniejszych problemach w dziedzinie ochrony prywatności i danych osobowych oraz szukać możliwych rozwiązań. **36. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności**, której gospodarzem był Urząd Ochrony Danych na Mauritiusie, była okazją do dyskusji, jak zapewnić bezpieczeństwo przetwarzanych danych i skutecznie chronić prywatność.

W dniach 13-14 października 2014 r. odbyła się sesja zamknięta Konferencji, przeznaczona wyłącznie dla rzeczników ochrony danych. Jej istotnym punktem było przyjęcie pięciu dokumentów, na które złożyły się 4 rezolucje oraz Deklaracja z Mauritiusa w sprawie Internetu Przedmiotów. 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.

W drugim dniu Konferencji odbyły się 4. warsztaty projektu PHAEDRA (14.10.2014 r.) „Further cooperation between DPAs, PCs and PEAs", poświęcone omówieniu kwestii związanych z kierunkami przyszłej współpracy i koordynacji działań na poziomie europejskim i międzynarodowym w zakresie egzekwowania prywatności[471]. Największy nacisk położony został na identyfikację barier ograniczających współpracę i koordynację działań w obszarze egzekwowania prawa do prywatności i ochrony danych osobowych oraz wskazano na konieczność opracowania 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. Podczas tego spotkania przedstawiona też została propozycja międzynarodowej umowy o współpracy w zakresie transgranicznego egzekwowania prawa oraz zarys nowego projektu PHAEDRA II.

Kolejne dwa dni Konferencji – 15 i 16.10.2014 r. – miały charakter otwarty i przebiegały z udziałem przedstawicieli wielu środowisk ze świata polityki, nauki, biznesu

[471] Więcej informacji na temat projektu można znaleźć na stronie internetowej http://www.phaedra-project.eu/, zaś program 4. warsztatów dostępny jest na stronie http://www.phaedra-project.eu/?page_id=49

oraz krajowych i międzynarodowych organizacji pozarządowych. Podczas tego wydarzenia Generalny Inspektor Ochrony Danych Osobowych przewodniczył sesji pt. „Przestępstwa gospodarcze, sztuczna inteligencja i roboty przeszukujące: profil nowoczesnego oszusta".

16. Warsztaty poświęcone ochronie danych (Praga, 9 listopada 2014 r.)

W dniu 9 listopada 2014 r. Generalny Inspektor Ochrony Danych Osobowych uczestniczył w Warsztatach pt. „Ochrona danych w związku z postępowaniami w sprawie oszustw korporacyjnych i zapobieganiem tego typu oszustwom" zorganizowanych przez Urząd Ochrony Danych Osobowych Republiki Czeskiej w Pradze. Podczas sesji poświęconej oszustwom korporacyjnym i ochronie danych Generalny Inspektor Ochrony Danych Osobowych wygłosił referat pt. „Czy potrzebne jest profilowanie obywateli? Dylematy prawa o ochronie prywatności".

9.5. Wizyty robocze.

1. Wizyta GIODO w siedzibie gruzińskiego organu ochrony danych.

W dniach 7-9 maja 2014 r. Generalny Inspektor Ochrony Danych Osobowych oraz jego przedstawiciel, gościli z wizytą w siedzibie nowo powstałego Urzędu Inspektora Ochrony Danych Osobowych Gruzji.

Celem wizyty było zapoznanie się z działalnością i funkcjonowaniem gruzińskiego organu ochrony danych oraz wymiana doświadczeń. Podczas spotkania Generalny Inspektor Ochrony Danych Osobowych przedstawił informacje na temat głównych priorytetów polskiego organu ds. ochrony danych, jak również podzielił się doświadczeniami m.in. w zakresie kontroli i podnoszenia świadomości obywateli na temat ochrony danych osobowych i prywatności.

2. Spotkanie GIODO z delegacją tokijskiego instytutu IISE.

W dniach 23-24 czerwca 2014 r. przebywała w Polsce delegacja tokijskiego instytutu IISE (Institute for International Socio-Economic Studies), przygotowująca raport dla rządu Japonii na temat wymiany danych osobowych w Polsce i Unii Europejskiej oraz w kontaktach z państwami spoza Europejskiego Obszaru Gospodarczego (EOG), w świetle najnowszych ustaleń Komisji Europejskiej (opinie WP 192 i WP 216) oraz najnowszych decyzji

Parlamentu Europejskiego. Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z delegacją tokijską odbyło się 24 czerwca 2014 r. w Gdańsku, podczas odbywających się w Trójmieście IV Dni Otwartych GIODO.

3. Wizyta delegacji Krajowej Agencji Ochrony Danych Osobowych Republiki Kosowa.

W dniach 7-10 lipca 2014 r. w Biurze GIODO gościła delegacja Krajowej Agencji Ochrony Danych Osobowych Republiki Kosowa. Wizyta studyjna odbyła się w ramach projektu UE „Wsparcie dla instytucji w Kosowie w obszarze ochrony danych osobowych". Spotkanie zapewniło uczestnikom możliwość zapoznania się z systemem ochrony danych osobowych w Polsce, jak również z funkcjonowaniem i działalnością polskiego organu ochrony danych. Przedstawiciele poszczególnych departamentów Biura GIODO przedstawili prezentacje poświęcone konkretnym kwestiom z zakresu ochrony danych, będących przedmiotem zainteresowania uczestników. Wizyta była również okazją do dyskusji i wymiany doświadczeń. Podczas tej wizyty podpisane zostało „Porozumienie o współpracy między polskim i kosowskim organem ochrony danych osobowych".

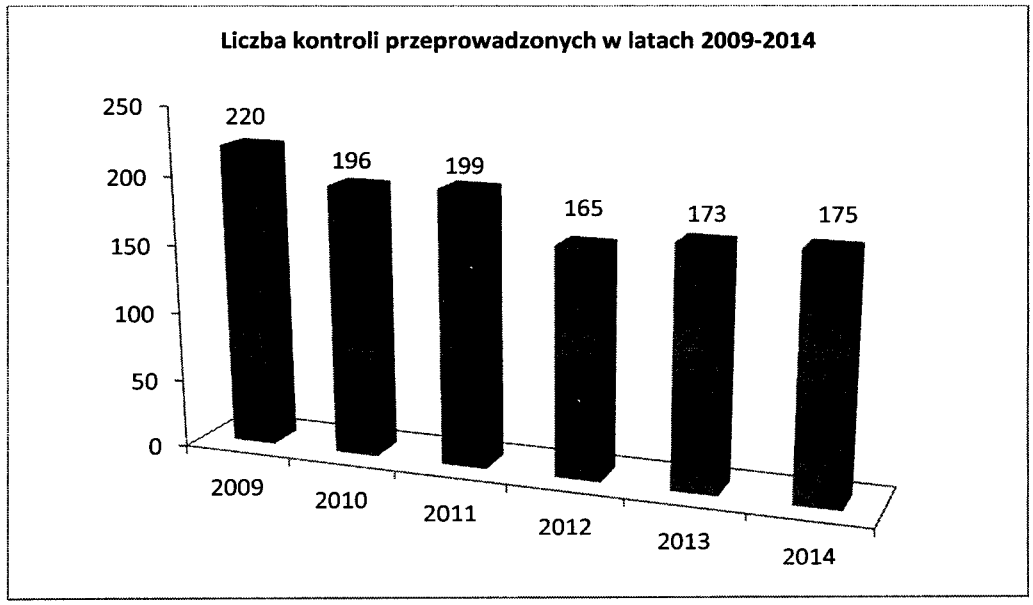
4. Wizyta przedstawicieli słowackiego Urzędu Ochrony Danych Osobowych.

W dniach 23-24 września 2014 r. w Biurze GIODO gościła delegacja słowackiego Urzędu Ochrony Danych Osobowych. Podczas tej wizyty przedstawiciele słowackiego 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.

Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2014 roku.

Charakteryzując działalność Generalnego Inspektora Ochrony Danych Osobowych w obszarze związanym z **kontrolą** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych, przypomnieć należy, iż w 2014 r. przeprowadzonych

zostało 175 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

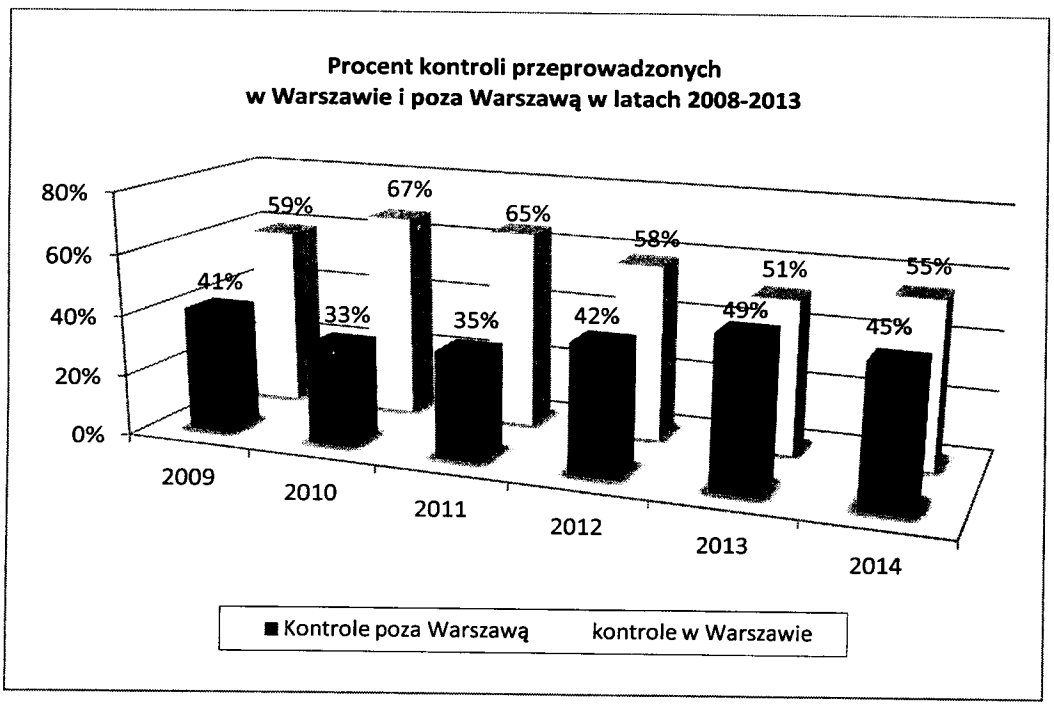


Wykres 34: ***Porównanie liczby kontroli przeprowadzonych w latach 2012–2014.***

Czynnościom kontrolnym poddane zostały m.in. szkoły wyższe, jednostki organizacyjne pomocy społecznej i jednostki obsługujące świadczenia rodzinne, powiatowe urzędy pracy, operatorzy pocztowi i podmioty świadczące usługi pocztowe realizowane na rzecz organów władzy publicznej, przewoźnicy, podmioty prowadzące hotele oraz podmioty prowadzące hurtownie farmaceutyczne. Dużą grupę jednostek kontrolowanych stanowiły również podmioty zaliczone do sektora „Inne", obejmującego te podmioty, które ze względu na charakter prowadzonej działalności nie mogły zostać zakwalifikowane do innej kategorii. W okresie sprawozdawczym szczególny nacisk położony został na przeprowadzenie tzw. kontroli sektorowych, którymi objęto w 2014 r. jednostki organizacyjne pomocy społecznej, jednostki obsługujące świadczenia rodzinne i powiatowe urzędy pracy w związku z wymianą informacji o osobach zarejestrowanych jako bezrobotne lub poszukujące pracy (11 kontroli), operatorów pocztowych i podmioty świadczące usługi pocztowe realizowane na rzecz organów władzy publicznej (12 kontroli), szkoły wyższe w związku z prowadzeniem domów studenckich (9 kontroli), przewoźników (13 kontroli), podmioty prowadzące hurtownie farmaceutyczne (14 kontroli) i hotele (5 kontroli). Wyniki przeprowadzonych kontroli zobrazowały sposób podejścia tych podmiotów 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 20 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.

W analizowanym 2014 roku na ogólną liczbę 175 kontroli, **96** z nich przeprowadzonych było w Warszawie (55%), zaś **79** poza Warszawą (45%).



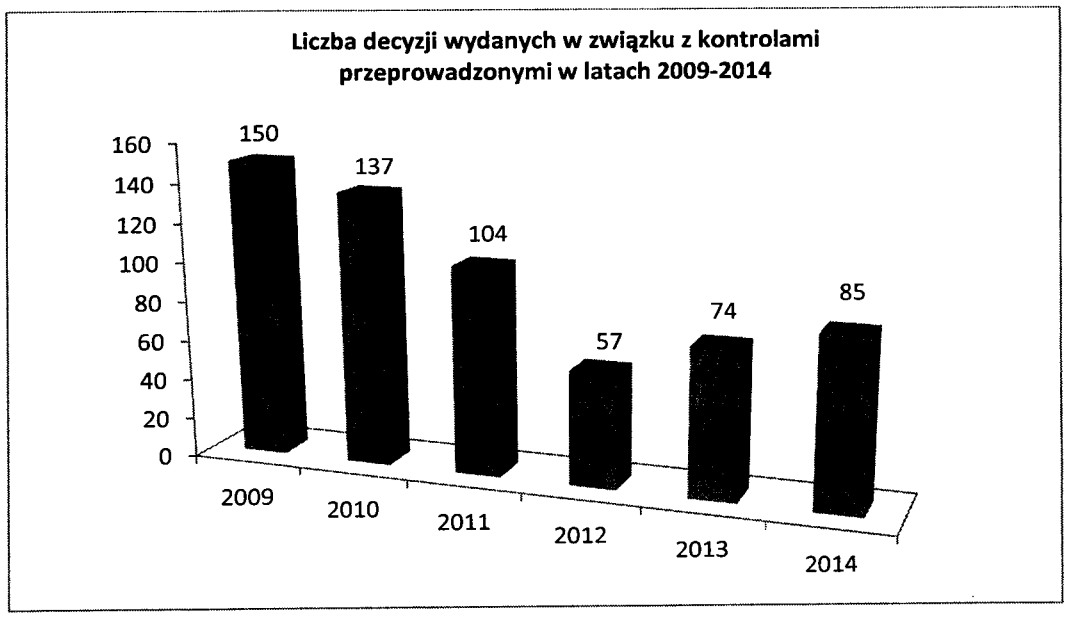
Wykres 35: ***Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2008–2013.***

Najwięcej kontroli przeprowadzonych zostało z urzędu (85). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący.

Inicjatywa kontroli	Liczba kontroli
Z urzędu	85
Departament Orzecznictwa, Legislacji i Skarg	55
Departament Rejestracji Zbiorów Danych Osobowych	11
Zespół ds. Naruszeń Danych Osobowych	1

Departament Edukacji Społecznej i Współpracy Międzynarodowej	1
Zespół ds. Egzekucji Administracyjnej	1
Policja	1
Prokuratura	4
Inspekcja Pracy	3
Naczelnik Urzędu Skarbowego	1
Związki zawodowe	1
W związku z inną kontrolą	11
RAZEM	**175**

W okresie sprawozdawczym w związku z przeprowadzonymi kontrolami wydanych zostało 85 decyzji administracyjnych.



Wykres 36: ***Decyzje wydane w związku z przeprowadzonymi kontrolami w latach 2012 – 2014.***

Oceniając wyniki przeprowadzonych kontroli należy stwierdzić, że część administratorów danych ma nadal 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

umieszczenie 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. Stwierdzano bowiem w toku kontroli, iż administratorzy danych pomimo istnienia przepisów prawa określających w sposób szczegółowy sposób przetwarzania danych osobowych, w tym dopuszczalny zakres zbierania danych osobowych, pozyskiwali od osób, których one dotyczą, dane wykraczające poza katalog danych zawarty w tych przepisach. Wskazać również należy, że zdarzały się przypadki, iż przekroczenie wynikającego z przepisów prawa dozwolonego zakresu przetwarzanych danych miało charakter istotnego naruszenia, gdyż było związane z pozyskaniem danych objętych szczególną ochroną na gruncie przepisów o ochronie danych osobowych, tj. danych o karalności. Administratorzy danych w dalszym ciągu mają także problemy z prawidłowym sformułowaniem treści oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych, tak aby wyrażona w taki sposób zgoda nie była domniemana lub dorozumiana z oświadczenia woli o innej treści. Analiza treści oświadczeń zebranych w toku kontroli niejednokrotnie wskazywała, że osobom składającym oświadczenie nie została zapewniona swoboda (możliwość wyboru) przy składaniu tych oświadczeń. Do częstych uchybień w tym zakresie należało również łączenie w jednym oświadczeniu zgód na różne cele przetwarzania danych i na rzecz kilku podmiotów.

Przeprowadzone kontrole wykazały również, że kontrolowane jednostki nadal mają problemy z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, 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 sprawozdaniu.

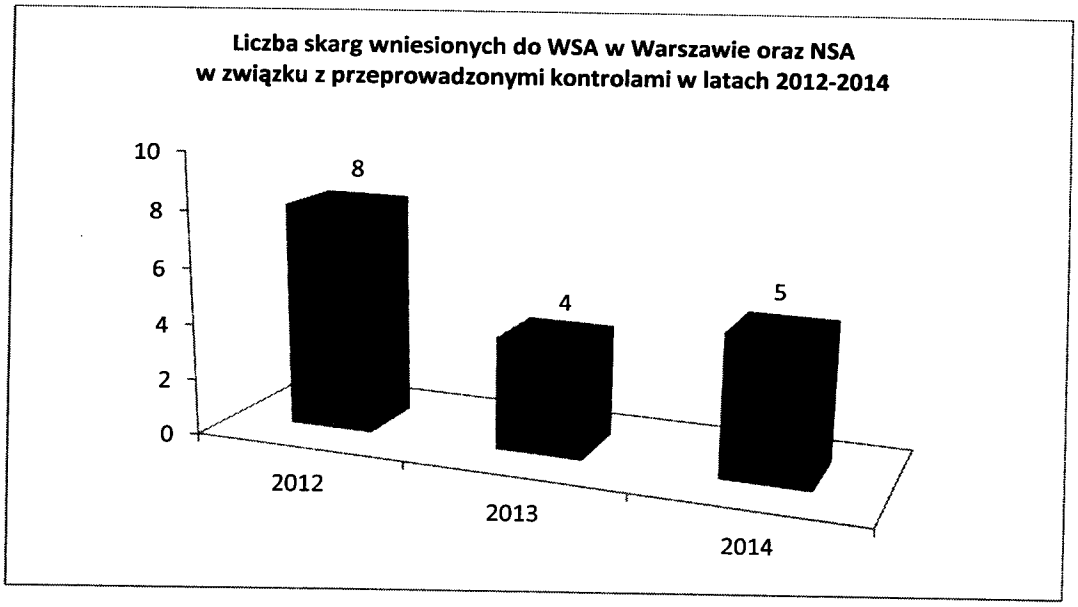
Obowiązki określone w przepisach o ochronie danych nie były wykonywane przez jednostki kontrolowane najczęściej z powodu błędnej interpretacji tych przepisów oraz ich niekonsekwentnego stosowania. Częstą przyczyną był również, jak wskazywali administratorzy danych, brak odpowiednich środków finansowych, 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 2014 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 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.

Na podstawie ustaleń z kontroli przeprowadzonych w 2014 r. należy stwierdzić, że w porównaniu z latami ubiegłymi osoby odpowiedzialne za przetwarzanie danych osobowych wykazały większą świadomość zagrożeń związanych z przetwarzaniem danych osobowych, a tym samym świadomość konieczności zapewnienia odpowiednich środków organizacyjnych i technicznych zapewniających ochronę tych danych. Konsekwencją było większe wyczulenie na prawidłowe dopełnienie obowiązków wynikających z przepisów o ochronie danych

osobowych. Niestety, powyższe spostrzeżenia nie dotyczą wszystkich podmiotów, w których przeprowadzono kontrole. Zdarzały się bowiem kontrole, które wykazywały, że jednostki kontrolowane nie wykonywały większości obowiązków wynikających z przepisów o ochronie danych osobowych. Innym negatywnym zjawiskiem zaobserwowanym w 2014 r. był brak współpracy podmiotu kontrolowanego z inspektorami dokonującymi czynności kontrolnych. Ten brak współpracy przejawiał się w szczególności trudnościami w umówieniu spotkania z osobami reprezentującymi jednostkę kontrolowaną celem okazania imiennych upoważnień i legitymacji służbowych uprawniających do przeprowadzenia kontroli oraz w długim czasie oczekiwania na osoby dysponujące wiedzą o procesie przetwarzania danych osobowych w celu przyjęcia od nich do protokołu ustnych wyjaśnień i na dokumenty mające bezpośredni związek z przedmiotem kontroli. Powyższy stan rzeczy ulega jednak stopniowej poprawie z uwagi na istnienie sankcji karnych za udaremnianie lub utrudnianie inspektorowi wykonania czynności kontrolnej[472].

W związku ze złożonymi skargami na decyzje wydane na skutek przeprowadzonych kontroli sądy administracyjne wydały sześć orzeczeń, w tym pięć orzeczeń wydał Wojewódzki Sąd Administracyjny w Warszawie, a jedno Naczelny Sąd Administracyjny.



Wykres 37: ***Skargi wniesione do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2012 – 2014.***

[472] Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Do istotnych orzeczeń, jakie zapadły w okresie sprawozdawczym w sprawach, w których przeprowadzane były kontrole, należy wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 kwietnia 2014 r. (sygn. akt II Sa/Wa 125/14). W tym wyroku Wojewódzki Sąd Administracyjny uchylił zaskarżoną decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie nakazu usunięcia uchybień w procesie przetwarzania danych osobowych, poprzez dopełnienie wobec osób, których dane pochodzą ze źródeł powszechnie dostępnych (Monitor Sądowy i Monitor Gospodarczy) i zostały zebrane i utrwalone przez ww. administratora danych, obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy o ochronie danych osobowych oraz stwierdził, iż decyzja ta nie podlega wykonaniu w całości. W uzasadnieniu wyroku WSA stwierdził, iż organ do spraw ochrony danych osobowych, dokonał ponownej analizy zebranego w sprawie materiału dowodowego, a nie przeprowadził - jak zalecił w wytycznych WSA - postępowania wyjaśniającego w sprawie w zakresie określonym w uzasadnieniu wyroku. Mimo, iż decyzja została zaskarżona tylko w części, sąd uznał, że wobec stwierdzonego uchybienia należało ją uchylić w całości, tym bardziej, że takie rozstrzygnięcie nie spowoduje dla spółki żadnych negatywnych konsekwencji.

Wojewódzki Sąd Administracyjny w Warszawie wydał w tej samej sprawie (sygn. akt II Sa/Wa 125/14) postanowienie z dnia 10 lutego 2014 r., o wstrzymaniu wykonania zaskarżonej decyzji Generalnego Inspektora Ochrony Danych Osobowych oraz utrzymaniu w mocy decyzji tego organu z dnia 24 września 2010 r. w części nakazującej spółce dopełnienie obowiązku informacyjnego. W uzasadnieniu postanowienia WSA stwierdził, iż strona uzasadniła żądanie zastosowania ochrony tymczasowej **oraz** wskazała, że w niniejszej sprawie zachodzą obie przewidziane w art. 61 § 3 ppsa[473] przesłanki uzasadniające wstrzymanie wykonania zaskarżonych decyzji Generalnego Inspektora Ochrony Danych Osobowych.

[473] Zgodnie z art. 61 § 3 prawo o postępowaniu przed sądami administracyjnymi, po przekazaniu sądowi skargi sąd może na wniosek skarżącego wydać postanowienie o wstrzymaniu wykonania w całości lub w części aktu lub czynności, o których mowa w § 1, jeżeli zachodzi niebezpieczeństwo wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków, z wyjątkiem przepisów prawa miejscowego, które weszły w życie, chyba że ustawa szczególna wyłącza wstrzymanie ich wykonania. Odmowa wstrzymania wykonania aktu lub czynności przez organ nie pozbawia skarżącego złożenia wniosku do sądu. Dotyczy to także aktów wydanych lub podjętych we wszystkich postępowaniach prowadzonych w granicach tej samej sprawy.

Do ważnych orzeczeń należy również wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 lipca 2014 r. (sygn. akt II Sa/Wa 2393/13), oddalający skargę naczelnika urzędu skarbowego na decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie rozstrzygnięcia, czy system monitoringu wizyjnego, pozwalający na identyfikację osób fizycznych, jest zbiorem danych osobowych podlegającym przepisom ustawy o ochronie danych osobowych. WSA oddalając skargę złożoną przez urząd skarbowy, potwierdził, że system monitoringu wizyjnego, pozwalający na identyfikację osób fizycznych, jest zbiorem danych osobowych i podlega przepisom ustawy o ochronie danych osobowych, a więc również obowiązkowi rejestracji w GIODO. Wojewódzki Sąd Administracyjny w Warszawie wydał również w tej sprawie postanowienie z dnia 4 marca 2014 r. w tej sprawie (sygn. akt II Sa/Wa 2393/13) odmawiając wstrzymania wykonania zaskarżonej decyzji Generalnego Inspektora Ochrony Danych Osobowych, w przedmiocie nakazu usunięcia uchybień w procesie przetwarzania danych osobowych. W uzasadnieniu postanowienia WSA w Warszawie stwierdził, iż z podanych przez stronę skarżącą okoliczności nie wynika, aby wykonanie zaskarżonej decyzji, rodziło niebezpieczeństwo wyrządzenia jej znacznej szkody i powstania sytuacji, w której brak będzie możliwości przywrócenia pierwotnego stanu rzeczy, czy też wynagrodzenia ewentualnej szkody.

W jednej ze spraw Wojewódzki Sąd Administracyjny w Warszawie postanowieniem z dnia 6 lutego 2014 r. (sygn. akt II Sa/Wa 144/14) odrzucił skargę spółki na decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie przetwarzania danych osobowych. Organ w uzasadnieniu wskazał, że skarga została złożona po terminie. Jak podkreślił, zgodnie z art. 53 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2012 r., poz. 270), skargę wnosi się w terminie trzydziestu dni od dnia doręczenia skarżącemu rozstrzygnięcia w sprawie. Strona skarżąca, mimo prawidłowego pouczenia, skargę wniosła z jednodniowym uchybieniem ustawowego terminu. Powyższe oznaczało, że skarga jest spóźniona i jako taka niedopuszczalna. Z tych też względów, WSA nie rozpatrzył wniosku strony skarżącej o wstrzymanie wykonania zaskarżonych decyzji.

Naczelny Sąd Administracyjny wyrokiem z dnia 21 lutego 2014 r. (sygn. akt I OSK 2445/12) przychylił się do stanowiska Generalnego Inspektora, wyrażonego w decyzji skierowanej do spółki, w której nakazano usunięcie uchybienia w procesie przetwarzania danych osobowych, poprzez wyznaczenie administratora bezpieczeństwa informacji. W uzasadnieniu wyroku NSA stwierdził, że z kodeksu cywilnego wynika, iż obowiązującą

regułą jest, że osoby prawne i jednostki organizacyjne niemające osobowości prawnej działają przez swoje organy, jeżeli innych reguł nie przyjmuje ustawa szczególna. Taka regulacja szczególna wynika z art. 36 ust. 3 ustawy o ochronie danych osobowych, jeżeli administratorem danych jest jednostka organizacyjna mająca lub niemająca osobowości prawnej, obowiązana jest wyznaczyć administratora bezpieczeństwa informacji. Ze względu na konstrukcję osób prawnych administrator danych osobowych będący osobą prawną ze swej istoty nie może samodzielnie wykonywać obowiązków administratora bezpieczeństwa informacji. Sąd podkreślił, że administrator danych osobowych, który nie wyznaczył administratora bezpieczeństwa informacji, nie może twierdzić, iż z mocy prawa wykonuje w takim przypadku obowiązki ABI samodzielnie. Należy przyjąć, że ABI powinien być osobą fizyczną, a w konsekwencji administrator danych może przejąć jego obowiązki tylko wtedy, gdy jest osobą fizyczną. Zgodnie z powyższym, spółka jest administratorem danych, która jest obowiązana wyznaczyć administratora bezpieczeństwa informacji.

W związku z przeprowadzonymi kontrolami Generalny Inspektor skierował w 2014 r. - do organów ścigania 3 zawiadomienia o podejrzeniu popełnienia przestępstwa opisanego w ustawie o ochronie danych osobowych. Do najistotniejszych należało zawiadomienie złożone w związku z ustaleniami dokonanymi w toku kontroli przeprowadzonej w Zarządzie Transportu Miejskiego z siedzibą w Warszawie (ZTM)[474]. Ww. kontrola wykazała, że ZTM, jako administrator danych, przekazał do Ministerstwa Finansów dane osobowe posiadaczy spersonalizowanej Warszawskiej Karty Miejskiej (dalej również: „WKM"), będących w przedziale wiekowym od 18 do 70 lat, ze zbioru danych o nazwie „Spersonalizowane Warszawskie Karty Miejskie", w celu dokonania weryfikacji w CRP KEP prowadzonym przez Ministra Finansów, czy osoby te posiadały na dzień 31 grudnia 2012 r. adres miejsca zamieszkania na terenie m.st. Warszawy, na potrzeby projektu Karta Warszawiaka i Karta Młodego Warszawiaka prowadzonego przez Prezydenta m.st. Warszawy, do czego nie miał podstaw prawnych. Z uwagi na powyższe, Generalny Inspektor skierował do **Prokuratury Rejonowej Warszawa - Wola zawiadomienie** o podejrzeniu popełnienia przez osoby odpowiedzialne za przetwarzanie danych osobowych w ZTM przestępstwa określonego w art. 49 ust. 1 ustawy o ochronie danych osobowych, polegającego na przetwarzaniu danych osobowych zgromadzonych zbiorze danych o nazwie „Spersonalizowane Warszawskie Karty Miejskie" w celu, dla którego ZTM nie był uprawniony te dane przetwarzać oraz czynu

[474] Sygn. akt DIS-K-421/3/14

określonego w art. 51 ust. 1 powołanej ustawy, polegającego na udostępnieniu danych osobowych z ww. zbioru osobom nieupoważnionym.

Postanowieniem z dnia 21 marca 2014 r. (sygn. akt 6 Ds. 113/14/V) Prokurator Prokuratury Rejonowej Warszawa – Wola odmówił wszczęcia dochodzenia w przedmiotowej sprawie. W uzasadnieniu postanowienia wskazano, iż w związku z tym, że cel przetwarzania danych przez ZTM był ściśle związany z prowadzoną działalnością administratora i odbiorcy danych, a administrator danych decydując się na przekazanie danych Ministrowi Finansów działał w interesie osób, których dane dotyczą, jako, że działania te miały na celu usprawnienie procesu przyznawania ulg i zniżek osobom korzystającym z transportu zbiorowego, to brak jest podstaw do przyjęcia, że postępowanie pracowników ZTM naruszało prawa i wolności posiadaczy kart miejskich. Wskazano, iż w niniejszym przypadku zastosowanie znajduje przesłanka legalizująca przetwarzanie danych osobowych wskazana w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych.

GIODO skierował zażalenie na ww. postanowienie do Sądu Rejonowego dla Warszawy - Woli. Postanowieniem z dnia 3 czerwca 2014 r. Sąd nie uwzględnił ww. zażalenia i utrzymał w mocy zaskarżone postanowienie Prokuratora Prokuratury Rejonowej Warszawa – Wola, podzielając stanowisko Prokuratora, iż przetwarzanie danych pochodzących ze zbioru danych o nazwie „Spersonalizowane Warszawskie Karty Miejskie" w celu weryfikowania uprawnień osób, których dane dotyczą, na potrzeby projektu Karta Warszawiaka i Karta Młodego Warszawiaka uzasadnione było przesłanką określoną w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych.

W wyniku kontroli przeprowadzonej w jednej ze spółek ustalono, że prowadziła ona serwis internetowy umożliwiający użytkownikom tego serwisu (przedsiębiorcom świadczącym usługi transportowe) udostępnianie pomiędzy sobą danych osobowych pochodzących ze zbiorów danych, których ww. użytkownicy są administratorami, w szczególności ze zbiorów danych kadrowych – dotyczących zatrudnienia kierowców. Za pośrednictwem tego serwisu dochodziło do wymiany informacji na temat kierowców, a także do ułatwienia im nawiązania kontaktu w celu przekazywania takich informacji, np. telefonicznie. Przedsiębiorca świadczący usługi transportowe (użytkownik serwisu), do którego zgłasza się kierowca poszukujący pracy, mógł na podstawie danych zawartych w jego życiorysie przeszukiwać bazę danych kierowców wprowadzonych do serwisu, w wyniku czego uzyskiwał dostęp do opinii o kierowcach (mogących potencjalnie być kandydatami do

pracy u przedsiębiorcy). Ww. przedsiębiorca dzięki serwisowi mógł skontaktować się bezpośrednio z użytkownikiem, który taką opinię zamieścił i uzyskać w ten sposób pełną informację o tożsamości kierowcy, którego opinia dotyczy. Do udostępnień między przedsiębiorcami świadczącymi usługi transportowe danych osobowych kierowców (obecnych lub byłych pracowników) dochodziło bez wiedzy tych kierowców.

Na podstawie ustalonego stanu faktycznego, w oparciu o obowiązujące przepisy[475], Generalny Inspektor Ochrony Danych Osobowych uznał, że podmiot, który dostarczył użytkownikom narzędzie w postaci serwisu internetowego, umożliwił udostępnianie osobom nieupoważnionym dane osobowe pochodzące ze zbiorów danych, których ww. użytkownicy są administratorami, w szczególności ze zbiorów danych kadrowych.

Z uwagi na powyższe, działając na podstawie art. 19 ustawy, Generalny Inspektor Ochrony Danych Osobowych skierował do **Prokuratury Rejonowej zawiadomienie** o podejrzeniu dopuszczenia się przez osoby odpowiedzialne za przetwarzanie danych osobowych w podmiocie, który dostarczył użytkownikom narzędzie w postaci serwisu internetowego, pomocnictwa w popełnieniu przestępstwa określonego w art. 51 ustawy, poprzez dostarczanie narzędzia w postaci serwisu internetowego umożliwiającego użytkownikom tego serwisu (przedsiębiorcom świadczącym usługi transportowe) udostępnianie osobom nieupoważnionym danych osobowych pochodzących ze zbiorów danych, których ww. użytkownicy są administratorami, w szczególności ze zbiorów danych kadrowych. Postanowieniem z dnia 31 października 2014 r. Prokurator Prokuratury Rejonowej umorzył dochodzenie w przedmiotowej sprawie.

W okresie sprawozdawczym Generalny Inspektor skierował ponadto do podmiotu kontrolowanego (marszałka województwa) wniosek o wszczęcie postępowania

[475] Art. 23 ust. 1 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. Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności: 1) marketing bezpośredni własnych produktów lub usług administratora danych, 2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej (art. 23 ust. 4 ustawy). Art. 26 ust. 1 pkt 2 ustawy. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2; zgodnie z ust. 2, przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje: 1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, 2) z zachowaniem przepisów art. 23 i 25 ustawy.

dyscyplinarnego wobec osób odpowiedzialnych za naruszenie przepisów o ochronie danych osobowych. Uzasadnieniem dla ww. wniosku były ustalenia dokonane w toku kontroli przeprowadzonej w urzędzie marszałkowskim jednego z województw, iż doszło do udostępnienia bez podstawy prawnej danych osobowych na stronie internetowej tego urzędu. W odpowiedzi marszałek województwa poinformował Generalnego Inspektora, że w wyniku wszczętego postępowania dyscyplinarnego osoby odpowiedzialne za udostępnienie danych osobowych, o którym mowa powyżej, zostały ukarane.

Natomiast odnosząc się do charakterystyki **pytań prawnych**, wskazać należy, iż w omawianym okresie sprawozdawczym do Biura Generalnego Inspektora wpłynęło ponad **4500 korespondencji z prośbami** o wyjaśnienie poszczególnych kwestii merytorycznych.

Większość podmiotów kierujących pytania do Generalnego Inspektora Ochrony Danych Osobowych (GIODO) nadal stanowiły osoby fizyczne, w tym prowadzące działalność gospodarczą. Z pewnością informacje potrzebne są w szczególności tym właśnie 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 – telefonicznie i w ramach codziennych konsultacji w siedzibie Biura. Statystyki w tych zakresach nie są prowadzone, mając jednak na uwadze liczbę odwiedzających Biuro GIODO osób, liczba porad ustnych wynosi ok. 700-1000 rocznie. Zauważyć także trzeba, że wciąż duża jest liczba zapytań nadsyłanych przez podmioty zawodowo zajmujące się udzielaniem porad prawnych (ok. 50, tj. ponad 1% ogółu wpływającej korespondencji). W tym przypadku należy domniemywać, iż zamiarem nadsyłających zapytania jest uzyskanie wykładni prawa, która mogła by być wykorzystana przez nich komercyjnie. Podnieść też należy, iż znaczna część nadsyłanej korespondencji nie dotyczy zagadnień, które powinny być rozpatrywane w aspekcie przepisów dotyczących ochrony danych osobowych, lecz innych dziedzin prawa, w szczególności cywilnego (np. ochrony dóbr osobistych, dochodzenia roszczeń), telekomunikacyjnego (np. metod zawierania i realizacji umów), dostępu do informacji publicznej (co podlega rozstrzygnięciom sądów), - czy kompetencji innych organów publicznych. Taka, *de facto* niezwiązana z działalnością GIODO korespondencja stanowi ponad 20% jej ogółu. Niepozostawanie zagadnienia w zakresie kompetencji Generalnego Inspektora Ochrony Danych Osobowych także wymaga wyjaśnienia nadsyłającemu pytanie, co rzecz jasna ogranicza możliwość wykorzystania pozostających w dyspozycji GIODO zasobów przewidzianych jedynie do celów ustawą o ochronie danych osobowych.

Podobnie jak w latach poprzednich, także w roku 2014, zakres tematyczny przesyłanych do Generalnego Inspektora Ochrony Danych Osobowych pytań pozostawał bardzo szeroki i dotyczył wszelkich aspektów przetwarzania danych osobowych, a także odnosił się do bardzo szerokiego kręgu podmiotów – zarówno z sektora prywatnego jak i publicznego – przetwarzających dane osobowe. Niemniej jednak można wskazać te zagadnienia, które pozostają, podobnie jak w latach ubiegłych, nadal aktualne. Dotyczą one w szczególności:

1) **Administracji i sądownictwa** – szczególnie interesujące i liczne były kwestie dotyczące upubliczniania, w tym na stronach internetowych, informacji o charakterze osobowym. W dalszym ciągu wiele wątpliwości dotyczyło pozyskiwania, w związku z prowadzoną działalnością, danych osobowych bez podstawy prawnej, lub w zakresie szerszym, niż przewidziany przepisami prawa, - jak również dostępu do informacji publicznej. W zakresie zaś sądownictwa, ujawniania wokand sądowych;
2) **Szkolnictwa** – np. dotyczące monitorowania losów absolwentów;
3) **Instytucji finansowych** – w przedmiocie ujawniania przez organy nadzoru finansowego informacji o złożonych zawiadomieniach o podejrzeniu popełnienia przestępstwa, wdrożenia ustawodawstwa FATCA, czy udostępnienia historii rachunku bankowego zmarłego klienta jego spadkobiercom;
4) **Służby Zdrowia** – w odniesieniu do podstaw przetwarzania danych o stanie zdrowia, w tym udostępnienia takich danych przez podmioty lecznicze innym podmiotom, np. Zakładowi Ubezpieczeń Społecznych;
5) **Zatrudnienia** – w zakresie dopuszczalnego zakresu danych oraz przesłanek legalizujących wykorzystywanie danych przez pracodawców, w tym przekazywania danych osobowych pracowników podmiotom zewnętrznym;
6) **Mieszkalnictwa** – zapytania dotyczące przetwarzania danych osobowych w związku z zarządzaniem nieruchomościami, w tym lokalami komunalnymi, wspólnotami mieszkaniowymi oraz przez spółdzielnie mieszkaniowe;
7) **Telekomunikacji i Internetu** - w tym w szczególności przechowywania informacji w postaci plików cookies, przetwarzania numerów IP komputerów, czy wykorzystania informacji stanowiących tajemnicę telekomunikacyjną na potrzeby postępowań sądowych;

8) **Monitoringu**, w tym wykorzystania urządzeń rejestrujących zarówno przez osoby fizyczne, jak i monitoringu wizyjnego stosowanego przez różnego rodzaju podmioty;
9) **Innych** zagadnień dotyczących ochrony danych osobowych – w tym wykorzystywania prywatnych nagrań np. zdarzeń drogowych, stosowania wideonadzoru (w szczególności przez podmioty publicznej służby zdrowia).

W omawianym okresie sprawozdawczym zauważalnym jest wzrost aktywności, czy prowadzenia różnorakiej działalności użytkowników Internetu, a co za tym idzie z tym związanego przetwarzania danych osobowych. Jednocześnie, łatwość użytkowania sieci wydaje się nie iść w parze ze wzrostem świadomości o wynikających z przepisów prawa obowiązkach dbałości o przetwarzane dane osobowe. Rozpoczynający działalność gospodarczą wydają się traktować tematykę ochrony danych osobowych jako „dodatek", nie zaś jej autonomiczną część. Tym samym liczba udzielanych porad prawnych w tym zakresie pozostaje w tendencji wzrostowej (ok. 350 w 2014 r.). Powszechna też informatyzacja życia publicznego powoduje niebezpieczną z punktu widzenia ochrony prywatności tendencję do budowania bardzo obszernych baz danych osobowych, w których przetwarzane mogą być częstokroć dane „na zapas", czy bez stosownej, precyzyjnej podstawy prawnej precyzyjnie regulującej daną działalność.

Praktyka wykorzystywania numeru PESEL jako jedynego identyfikatora użytkownika, czy klienta jest coraz częściej stosowana w sposób nieuzasadniony. W większości bowiem przypadków można by posłużyć się inną daną, np. specjalnie wytworzonym identyfikatorem, hasłem, nie przetwarzając danych osobowych zbędnych dla funkcjonalności określonego systemu.

Istotną tematyką pozostaje szeroko rozumiane **mieszkalnictwo**. Odnośnie wspólnot i spółdzielni mieszkaniowych warto w tym miejscu zauważyć, iż w omawianym okresie sprawozdawczym do Biura Generalnego Inspektora Ochrony danych Osobowych wpłynęło około 40 próśb o interpretację przepisów prawa od samych spółdzielni, i ok. 100 zapytań prawnych dotyczących spółdzielni. W przypadku wspólnot mieszkaniowych natomiast, około 60 pytań dotyczyło ich działalności. Tematycznie natomiast zauważalna jest duża powtarzalność niniejszych. Bardzo wiele zagadnień dotyczyło chociażby legalności udostępnienia wynagrodzeń osób zarządzających spółdzielniami i wspólnotami, praw lokatorów dotyczących wglądu do umów, czy wywieszania informacji dotyczących zadłużenia członków spółdzielni i wspólnot na klatkach schodowych. Sprawy te były

sukcesywnie omawiane w sprawozdaniach GIODO z lat poprzednich, sukcesywnie też uzupełniana jest pod kątem nowych zagadnień strona internetowa Generalnego Inspektora tak, aby na podstawie udzielanych odpowiedzi na zapytania zachowywała ona aktualność pod kątem nowych zagadnień związanych z przetwarzaniem danych osobowych w tych podmiotach.

Wciąż wiele kontrowersji związanych jest z powszechnie już wykorzystywanym wideonadzorem. W około bowiem 50 przypadkach Generalny Inspektor zajmował stanowiska w tego typu sprawach wobec administratorów danych. W związku z rozpowszechnieniem urządzeń służących monitoringowi istotną kwestią pozostaje konflikt pomiędzy prawem do stosowania takich rozwiązań do celów osobistych osób prywatnych a innymi osobami, gdy stosowanie takich rozwiązań okazuje się jednak ingerencją w interesy chociażby lokalnych społeczności.

Powyżej przytoczone przykłady pozostają oczywiście jedynie częścią tematyki wpływających do Biura GIODO zagadnień obejmującej wszakże wszystkie właściwie dziedziny życia publicznego. Z natury rzeczy więc duża cześć z nich nie dotyczy w istocie kompetencji Generalnego Inspektora, lecz także działalności innych podmiotów publicznych. Każdorazowe natomiast ukierunkowanie obywatela lub podmiotu treścią udzielonej mu odpowiedzi na konkretną, opartą na przepisach prawa szczególnych względem ustawy o ochronie danych osobowych dziedzinę, okoliczność, czy działalność, pozwala odnaleźć się, umiejscowić problem we właściwych sferach czy strukturach. Takie zaś umiejscowienie z kolei pozwala niejednokrotnie uniknąć prowadzenia zbędnych, kosztownych z punktu widzenia państwa postępowań administracyjnych, i to zarówno przed organem do spraw ochrony danych osobowych, jak i innymi podmiotami publicznymi. Tę kwestię podnieść należy dlatego, iż forma działalności edukacyjnej – odpowiedzi na pytania, nie została określona w przepisach kompetencyjnych Generalnego Inspektora. Przepisy te nie stanowiąc obowiązku udzielania odpowiedzi nie reglamentują tej formy działalności przepisami chociażby Kodeksu postępowania administracyjnego, absorbują natomiast skromne zasoby Generalnego Inspektora stanowiąc jednocześnie najbliższą obywatelowi i najprostszą zarazem formę kontaktu z organem opartego na zasadzie pisemności.

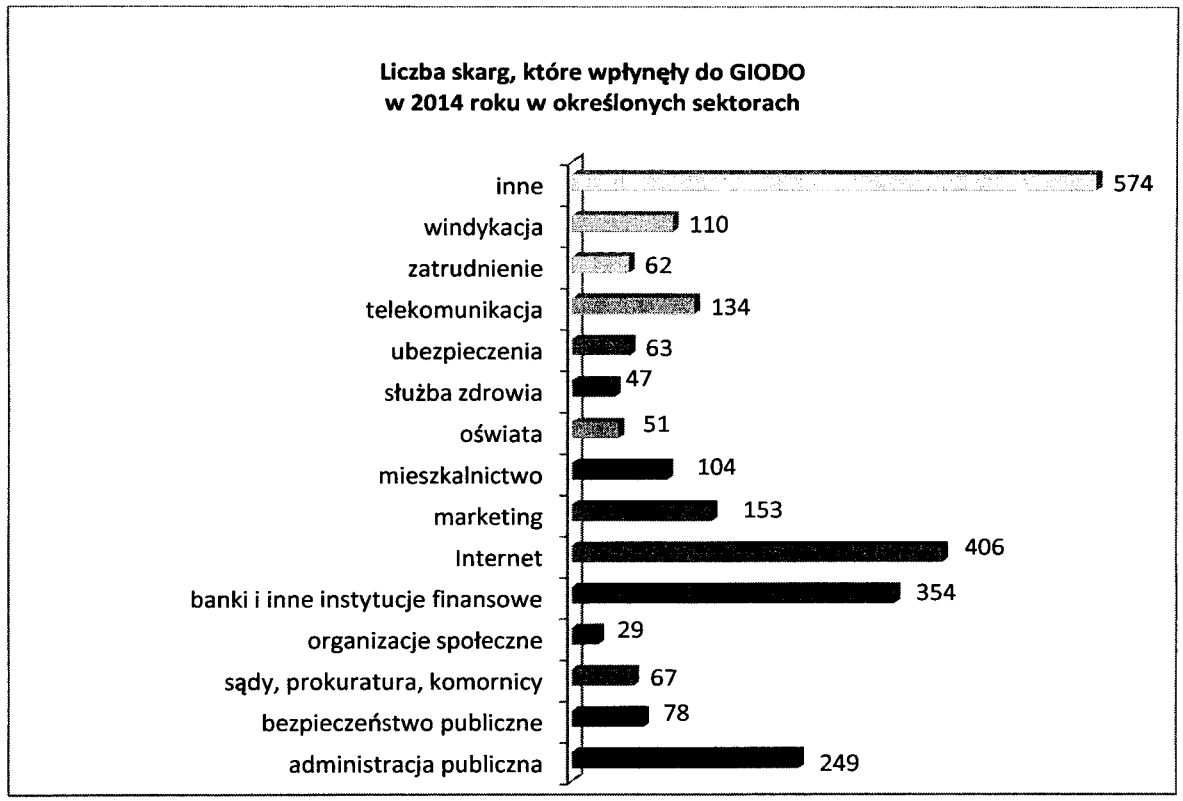
W ramach realizacji swoich ustawowych uprawnień oraz mając na uwadze potrzebę ciągłego doskonalenia ochrony danych osobowych, Generalny Inspektor Ochrony Danych Osobowych kieruje **wystąpienia do podmiotów publicznych i prywatnych, sygnalizując w nich konieczność zmiany stosowanych przez te podmioty 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 2014 Generalny Inspektor Ochrony Danych Osobowych wystosował **66 wystąpień.**

W porównaniu z poprzednimi latami, w 2014 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, w 2013 – 1879, **zaś w 2014 r. – 2481.** 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 - 2013-2014 pozwala zauważyć interesujące trendy. Pierwszym z nich był znaczący wzrost liczby skarg w sektorze dotyczącym Internetu (rok 2013- 224, rok 2014 - 406), w sektorze odnoszącym się do działalności banków i innych instytucji finansowych (rok 2013- 247, rok 2014 – 354), jak również w zakresie działalności marketingowej (rok 2013 – 93, rok 2014 – 153)). Znaczący wzrost liczby skarg, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych nastąpił w również w sektorze dotyczącym zatrudnienia (rok 2013- 23, rok 2014 – 62). Ponadto znaczący spadek odnotowano jeśli chodzi o liczbę skarg, które wpływają do biura GIODO w sektorze dotyczącym organizacji społecznych (rok 2013- 63, rok 2014 - 29). Zaakcentować należy, iż w niektórych sektorach liczba skarg była na porównywalnym poziomie, tj. w sektorze dotyczącym administracji publicznej (rok 2013- 236, rok 2014 - 249), w sektorze bezpieczeństwa publicznego (rok 2013- 72, rok 2014 - 78), - w sektorze dotyczącym służby zdrowia (rok 2013 – 48, rok 2014 - 47) oraz w sektorze dotyczącym mieszkalnictwa (rok 2013- 93, rok 2014 - 104).



Wykres 43: ***Porównanie liczby skarg, które wpłynęły do Biura GIODO w 2014 r. w poszczególnych sektorach.***

W podsumowaniu należy zauważyć, że systematycznie poprawia się poziom przetwarzania danych osobowych przez administratorów danych, którzy – jak wynika z podejmowanych przez nich działań – współdziałają z organem ochrony danych osobowych w celu wypracowywania lepszych standardów ochrony danych. W wielu sprawach bowiem, po interwencji Generalnego Inspektora, podejmowali oni odpowiednie działania zmierzające do zmian kwestionowanych praktyk.

Odnosząc się do faktu corocznego wzrostu liczby wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych **skarg** związanych z przetwarzaniem danych osobowych, należy wskazać, że przyczyną powyższego jest nie tylko fakt naruszania ustawy - o ochronie danych osobowych przez administratorów danych, ale także coraz większa świadomość osób, których dane dotyczą odnośnie przepisów dotyczących ochrony danych osobowych. Jednym z istotnych czynników w tym zakresie był niewątpliwie wzrost aktywności ludzi w sieci Internet, który spowodował prawie dwukrotny wzrost skarg. Ponadto wzrost skarg wynikał również z braku właściwej identyfikacji przez skarżących zasad

powierzania przetwarzania danych, które nie prowadzi do zmiany statusu administratorów danych osobowych.

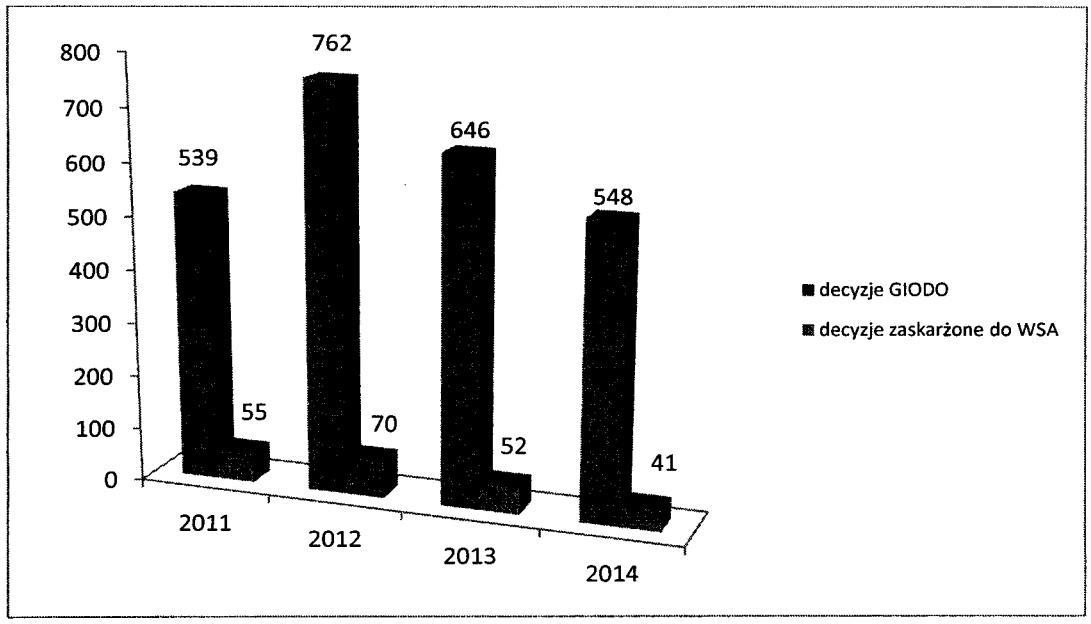
Można zaobserwować wzrost świadomości po stronie administratorów danych osobowych w przypadku dużych podmiotów gospodarczych, które traktują politykę bezpieczeństwa danych swoich klientów jako jeden z ważniejszych elementów ich pozytywnego wizerunku. Odnosząc się do drobnych przedsiębiorców, czy podmiotów pożytku publicznego można zauważyć, że często nie są świadomi faktu, że są administratorami danych osobowych i że spoczywają na nich konkretne obowiązki określone przez przepisy prawa.

W przedmiocie naruszeń przepisów ustawy o ochronie danych osobowych można zaobserwować, iż najczęściej występującym naruszeniem był brak spełniania przez administratorów danych osobowych obowiązków informacyjnych wynikających z art. 33 ustawy. Ponadto zaobserwowany został problem niespełniania przez banki własnego obowiązku informacyjnego z art. 105 ust. 3 ustawy Prawo bankowe. Każdorazowo w takich sytuacjach GIODO podejmował czynności mające na celu wyeliminowanie zaobserwowanych nieprawidłowości.

Podsumowując należy odnotować, iż mimo dużej liczby skarg, które wpłynęły do GIODO w 2014 r., w stosunku do lat ubiegłych 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.

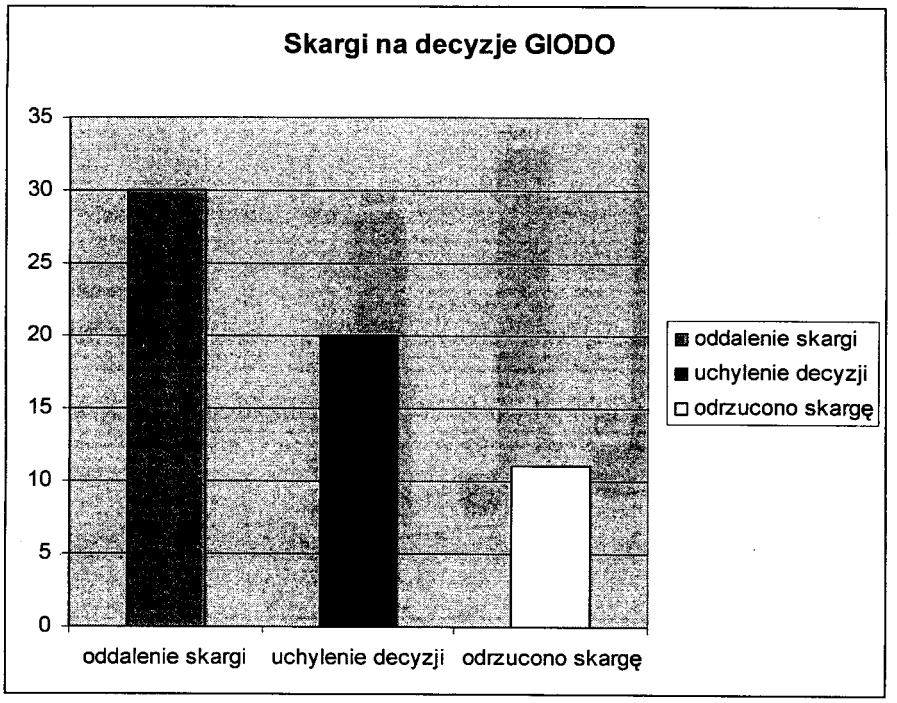
Odnosząc się do zakresu tematycznego rozpatrywanych w omawianym 2014 roku skarg przez Generalnego Inspektora Ochrony Danych Osobowych zasadniczo nie zauważa się znaczących zmian. W porównaniu z rokiem 2013 problemy pojawiające się we wpływających do Biura Generalnego Inspektora wnioskach uznać należy za tożsame.

W postępowaniach zainicjowanych skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, w roku 2014 r., spośród **547** decyzji wydanych przez Departament Orzecznictwa, Legislacji i Skarg, **41** spośród nich zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [WSA]. W porównaniu z rokiem 2013, w którym 52 decyzji zostało zaskarżonych, oznacza to **spadek o 11**.



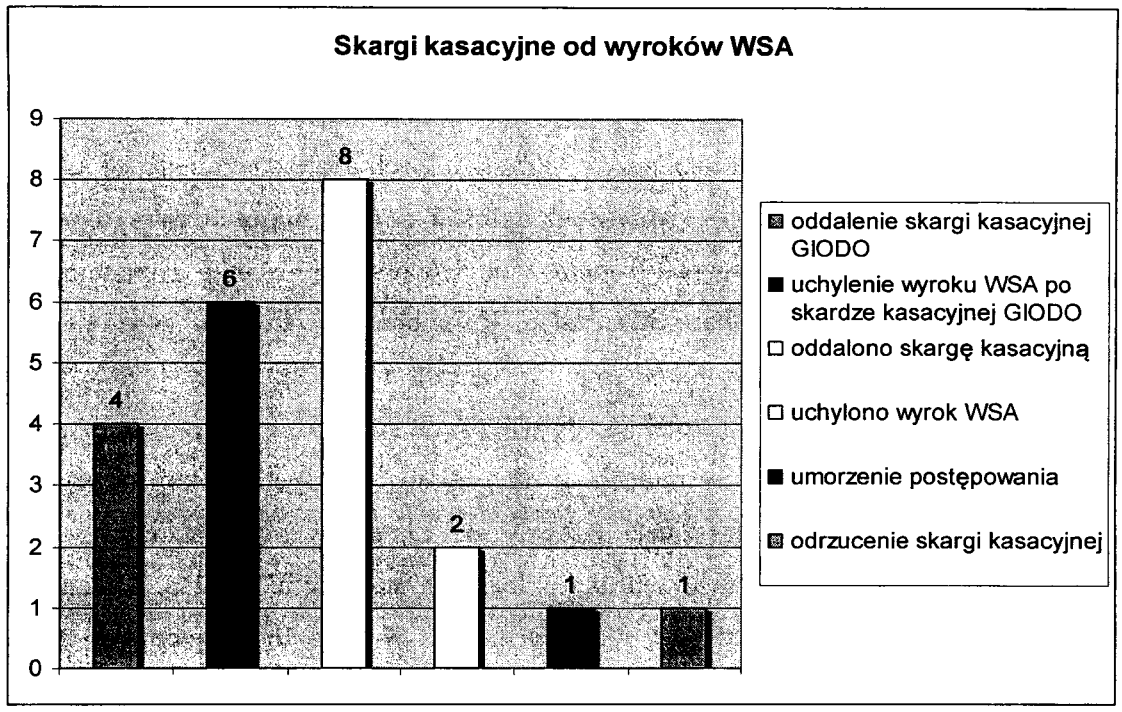
Wykres 39: ***Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2013 w związku z rozpatrywanymi skargami.***

Spośród 188 orzeczeń wydanych w sprawach związanych z działalnością skargową DOLiS 120 orzeczeń rozstrzygało sprawy co do istoty, zaś pozostałych 68 orzeczeń stanowiły orzeczenia wydawane w toku prowadzonych przez sądy administracyjne postępowań.



Wykres 40 ***Orzeczenia WSA wydane w 2014 r. w sprawach prowadzonych przez Generalnego Inspektora. W analizowanym okresie WSA rozstrzygał sprawy co do istoty w 98 przypadkach.***

Wśród orzeczeń wydanych przez WSA dotyczących skarg na decyzje GIODO w 2014 r. w **30** przypadkach Sąd orzekł o **oddaleniu** skargi na decyzję GIODO, zaś w **20** przypadkach **uchylił** zaskarżone decyzje. Ponadto w **11** sprawach WSA orzekł o **odrzuceniu** skargi spowodowanym nieuzupełnieniem, we wskazanym przez Sąd terminie, braków formalnych złożonych skarg. Podkreślić należy, iż w **10** sprawach GIODO kierował do NSA skargi kasacyjne od wyroków WSA na skutek których w **6** sprawach zostały uchylone wyroki WSA, zaś w **4** przypadkach oddalono skargi kasacyjne GIODO. Spośród skarg kasacyjnych skarżących podkreślić należy, iż w **8** przypadkach zostały one oddalone, w **2** sprawach wyroki WSA zostały uchylone, zaś po **1** sprawa została umorzona i **1** skarga kasacyjna została odrzucona.



Wykres 41. ***Orzeczenia NSA w 2014 r. w związku ze skargami kasacyjnymi wniesionymi od wyroków WSA.***

Analizując z kolei działalność **opiniotwórczą** Generalnego Inspektora Ochrony Danych Osobowych w 2014 r. zauważyć należy, iż proces legislacyjny wymaga udziału jego przedstawicieli w różnego rodzaju etapach prac, począwszy od sporządzenia opinii GIODO - na piśmie, poprzez udział w komisjach uzgodnieniowych organizowanych przez projektodawców, celem utrzymania uwag GIODO, aż po udział w pracach Parlamentu, w przypadku przepisów o randze ustawy.

Za istotne osiągnięcie Generalnego Inspektora Ochrony Danych Osobowych w obszarze legislacji uznać należy doprowadzenie – we współpracy z innymi podmiotami - do zaniechania przez Ministerstwo Sprawiedliwości prac dotyczących projektu **ustawy o oświadczeniach o stanie majątkowym osób pełniących funkcje publiczne**. Podnieść wypada, iż organ do spraw ochrony danych osobowych skrytykował podstawowe założenia powyższego projektu jako naruszające konstytucyjne prawa obywateli. Ten pogląd Generalnego Inspektora podzieliło kilkanaście innych podmiotów i organizacji, które w swoich uwagach podnosiły podobne zarzuty.

Za równie istotne osiągnięcie należy uznać przedstawienie uwag do projektu **ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz niektórych innych ustaw**.

Skierowanie tej ustawy do Trybunału Konstytucyjnego z wnioskiem o zbadanie jej zgodności z Konstytucją Rzeczypospolitej Polskiej w trybie tzw. kontroli prewencyjnej, organ do spraw ochrony danych osobowych uznaje za całkowicie słuszne i zasadne.

Zainteresowaniem organu do spraw ochrony danych osobowych będą się nadal również cieszyły prace nad **rządowym projektem założeń ustawy o ponownym wykorzystaniu informacji sektora publicznego**. Pismem z dnia 6 czerwca 2014 r. Generalny Inspektor zgłosił uwagi do tego projektu zaznaczając, iż najbardziej istotnym zagadnieniem, jakie pojawiło się przy tej regulacji ustawowej – ze wszech miar potrzebnym – zasad ponownego wykorzystania informacji publicznej jest potwierdzenie, że informacja publiczna gromadzona przez podmioty publiczne w ramach i dla celów zgodnych z konstytucyjną zasadą praworządności, będzie w przyszłości przetwarzana dla celów zupełnie innych, nad którymi organy władzy publicznej stracą kontrolę. Z tego też względu niezbędne jest czuwanie, aby informacje te, wykorzystywane już w innych celach, nie naruszały przepisów regulujących ochronę danych osobowych.

Należy również wskazać, iż ustawa z dnia 28 listopada 2014 r. **Prawo o aktach stanu cywilnego** (Dz. U. z 2014 r. poz. 1741), która weszła w życie 1 marca 2015 r. uwzględniła w większości uwagi Generalnego Inspektora. W zakresie postulowanym przez GIODO przepisy dotyczące sporządzania nowego aktu stanu cywilnego w określonych przypadkach uzupełniono o wyraźny zakaz ujawniania dotychczasowego aktu stanu cywilnego.

Organ do spraw ochrony danych osobowych oczekuje także na dalsze prace nad **projektem założeń ustawy o monitoringu wizyjnym.** Druga wersja projektu przedstawiona przez Ministerstwo Spraw Wewnętrznych zawierała uporządkowaną strukturę propozycji legislacyjnych, które - jednakże w sposób niewystarczający - określały uprawnienia osób obserwowanych, oznaczenia przestrzeni monitorowanych, jak również zakres udostępniania nagrań z monitoringu. Generalny Inspektor Ochrony Danych Osobowych, podobnie jak projektodawca, ma nadzieję na szybkie zakończenie prac nad trzecią wersją projektu, która w sposób prawidłowy będzie gwarantowała konstytucyjne wolności i prawa jednostki.

W odniesieniu do prac nad **projektem założeń projektu ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji oraz niektórych innych ustaw**, w dniu 24 lutego 2015 r. Prezes Rady Ministrów poinformował o odroczeniu rozpatrzenia powyższego projektu założeń.

Natomiast w odniesieniu do **projektu założeń projektu ustawy o zmianie ustawy o udostępnianiu informacji gospodarczych i wymianie informacji gospodarczych**, Rada

Ministrów przyjęła założenia, postanawiając o wyłączeniu z dokumentu fragmentu odnoszącego się do pozyskiwania danych z rejestru dłużników publicznoprawnych, którego powstanie przewiduje – wskazany powyżej – **projekt założeń projektu ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji**.

Wskazać należy, iż zauważalna jest tendencja do cyfryzacji społeczeństwa. Rozumiejąc, iż państwo zmierza do usprawnienia procesów zarządzania posiadanymi systemami i zgromadzonymi w nich danymi, jak również zapewnić łatwiejszy dostęp obywatela do usług tzw. e-administracji, zastanowienia często wymaga – i o to postuluje GIODO w swoich opiniach do poszczególnych projektów przepisów, czy też do założeń określonych rozwiązań - czy projektodawcy aktów prawnych w należyty sposób odnoszą się do zastosowania rozwiązań alternatywnych (to jest nie wykorzystujących danych osobowych w nadmiarze) na etapie założeń czy projektów aktów prawnych. Idea cyfryzacji często prowadzi bowiem do zbyt dużych uproszczeń w procedurach przetwarzania danych osobowych, co narażać może nie tylko na pogwałcenie obowiązujących w porządku prawnym zasad, ale także do niebezpiecznych sposobów przetwarzania danych osobowych. Wśród konsekwencji nienależytego trybu postępowania dotyczącego danych osobowych wymienić należy: udostępnianie danych osobom nieupoważnionym, utratę czy kradzież tychże danych, jak również gromadzenie konkretnych rodzajów danych w przypadku, gdy wymagane są jedynie dane statystyczne.

Refleksje organu do spraw ochrony danych osobowych - po przeanalizowaniu projektów, które wpłynęły do Biura GIODO w 2014 r. zmierzają w kierunku stwierdzenia, iż mimo obowiązywania ustawy o ochronie danych osobowych od 1997 r. nadal istnieje potrzeba korygowania zachowań zmierzających do pozyskiwania w aktach powszechnie obowiązującego prawa danych osobowych zbędnych, nieadekwatnych, nadmiernych do przyjmowanych rozwiązań. Wiele z przedstawianych organowi do spraw ochrony danych osobowych do zaopiniowania rozwiązań nie przechodzi testu konstytucyjności, jeśli chodzi o niezbędność, adekwatność, proporcjonalność czy też cel pozyskiwanych danych osobowych w stosunku do ich zakresu. Brak właściwego uzasadnienia niezbędności przyjęcia rozwiązań coraz bardziej ingerujących w prywatność prowadzi do powstania niezgodnych zarówno z art. 51 Konstytucji, jak i ustawą o ochronie danych osobowych rozwiązań. Projektodawcy tworzą ponadto akty wykonawcze, podczas gdy niezbędne jest wdrażanie rozwiązań ustawowych, o czym odpowiednie podmioty zdają się zapominać, a Generalny Inspektor Ochrony Danych Osobowych musi korygować powyższe działania. Często mają miejsce sytuacje, w których

regulowanie przetwarzania danych osobowych podlegających szczególnej ochronie – zgodnie z art. 27 ustawy o ochronie danych osobowych – ma miejsce w rozporządzeniach, a nie w ustawie. Zauważyć ponadto należy, iż nie w każdym przypadku projekty aktów prawnych są przesyłane do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych, co w praktyce powoduje uchwalanie i wydawanie przepisów niezgodnych z zasadami ochrony danych osobowych.

Mając na względzie projekty aktów prawnych, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w okresie sprawozdawczym, zauważalna jest tendencja do tworzenia przez poszczególne resorty zintegrowanych baz danych lub łączenia kilku baz danych zawierających dane osobowe w jeden system. Proponowane są rozwiązania, które niestety nie przeszły wcześniej testu wpływu na prawo do prywatności. Brak wcześniejszej oceny wielu aktów prawnych na etapie koncepcji przyjmowanych w nich rozwiązań (zarówno prawnych, proceduralnych jak i technicznych) nie sprzyja jakości stanowionego prawa. Każde przetwarzanie danych osobowych powinno być planowane **z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania (*privacy by design*)**, co stara się wskazywać jak najczęściej Generalny Inspektor w swoich opiniach do projektu. Informuje projektodawców, że idea *privacy by design* zrodziła się jako sposób spojrzenia na budowanie systemów teleinformatycznych. Polega ona na tym, by od samego początku tworzenia jakiegoś systemu, na każdym etapie, rozważać wpływ tworzonych rozwiązań na sferę prywatności i nie tyle odpowiadać na pojawiające się problemy, co już wcześniej przewidywać najważniejsze z nich i im przeciwdziałać. Zasada ochrony prywatności w fazie projektowania została zawarta również w przepisach procedowanego obecnie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Opierając się na doświadczeniach wynikających z opiniowania aktów prawnych w 2014 r. wskazać należy, iż funkcjonowanie projektowanych przez poszczególne resorty systemów informatycznych nie znajduje swojego odzwierciedlenia ani w przepisach rangi ustawy, ani w aktach wykonawczych. Brakuje również oceny wpływu tychże systemów na zakres przetwarzanych w nich danych. Zauważyć należy, iż szereg unormowań uwzględniających dane osobowe jest regulowanych przez podmioty prawa publicznego w formie porozumień czy umów o współpracy, podczas gdy zasady związane z ograniczaniem prawa do samostanowienia jednostki powinny być wyłącznie wytyczane materią ustawową.

Wśród pojawiających się wyzwań na kolejny rok wskazać należy, iż koniecznym będzie uregulowanie takich obszarów jak biometria, sposoby przetwarzania informacji pozyskiwanych przez drony, czy też korzystanie z monitoringu (wizyjnego z rejestracją dźwięku), gdyż takie rozwiązania zaczynają być proponowane w przekazywanych Generalnemu Inspektorowi projektach. Niezależnie od rozwijających się nowych technologii przetwarzania danych osobowych, organ powołany do ich ochrony stoi i będzie stać na straży zgodnego z prawem, w tym z zasadami konstytucyjnymi, i adekwatnego w stosunku do celów przetwarzania danych, wykonywania na tych danych operacji ograniczonych w czasie, oraz zapewniać jednoznaczność interpretacji obowiązujących przepisów prawa.

Jak już była o tym mowa, w 2014 r. zgłoszonych zostało do **rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych 43300 zbiorów, z czego 26703 zbiory pochodziły od podmiotów publicznych, zaś 16597 od podmiotów prywatnych.**

W przypadku sektora publicznego, odnotowany znaczący wzrost liczby zgłoszeń zbiorów danych osobowych przesyłanych do rejestracji GIODO spowodowany był wejściem w życie w omawianym okresie sprawozdawczym nowych regulacji prawnych, skutkujących tworzeniem przez jednostki samorządu terytorialnego nowych zbiorów danych w związku z realizacją przypisanych im zadań i kompetencji. Jako przykład można wskazać ustawę z dnia 4 kwietnia 2014 r. o ustaleniu i wypłacie zasiłków dla opiekunów (Dz. U. z 2014 r. poz. 567), która określiła warunki nabywania oraz zasady ustalania i wypłacania zasiłków dla opiekunów, czy też rozporządzenie Rady Ministrów z dnia 27 maja 2014 r. w sprawie szczegółowych warunków realizacji rządowego programu dla rodzin wielodzietnych (Dz. U. z 2014 r. poz. 755). Natomiast wśród zgłoszeń do rejestracji pochodzących od podmiotów publicznych w roku 2014 r. (podobnie jak w latach poprzednich) stosunkowo dużą liczbę stanowiły zbiory danych osobowych zgłaszane do rejestracji przez przedszkola i szkoły. Nową kategorię zbiorów tworzonych w ramach szeroko rozumianego systemu oświaty, związanych z nowymi przepisami wprowadzonymi ustawą z dnia 6 grudnia 2013 r. o zmianie ustawy o systemie oświaty oraz niektórych innych ustaw (Dz. U. z 2014 r. poz. 7), stanowiły zgłaszane przez gminy i ośrodki pomocy społecznej zbiory prowadzone w związku z weryfikacją oświadczeń składanych w toku realizacji prowadzonej przez jednostki oświatowe.

W tym miejscu warto podkreślić, że w związku z rozwojem świadomości prawnej administratorów danych w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych, od kilku lat można zaobserwować skokową tendencję wzrostu liczby

zgłoszeń zbiorów danych osobowych przesłanych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Wiąże się to także z wciąż rosnącą świadomością obywateli w zakresie przysługujących im, w związku z przetwarzaniem dotyczących ich danych osobowych, uprawnień, a jawny rejestr zbiorów danych osobowych stanowi dla nich istotne narzędzie pozwalające efektywnie z tych praw korzystać. Wzrasta tym samym znaczenie funkcji informacyjnej rejestru zbiorów danych osobowych.

Co więcej, postępowania rejestracyjne prowadzone przez Generalnego Inspektora Ochrony Danych Osobowych mają także istotny walor edukacyjny. Obowiązek zgłoszenia zbioru danych do rejestracji GIODO oraz świadomość skutków jej ewentualnej odmowy niewątpliwie mobilizuje administratorów danych do tego, aby już na etapie wypełniania zgłoszenia dokonali oceny, czy spełnili wszystkie wymagania przewidziane w ustawie o ochronie danych osobowych. W toku prowadzonych postępowań rejestracyjnych funkcja edukacyjna realizowana jest przede wszystkim poprzez wyjaśnienie administratorowi zasad dotyczących przetwarzania danych osobowych, przedstawienie interpretacji Generalnego Inspektora Ochrony Danych Osobowych oraz orzecznictwa sądów administracyjnych dotyczącego przepisów o ochronie danych osobowych. W 2014 r. wysłano do administratorów danych około 2 tysięcy pism zawierających tego rodzaju informacje. Skutek edukacyjny będzie miał również wpływ na prawidłowe prowadzenie również innych zbiorów tworzonych przez danego administratora danych.

Warto zwrócić uwagę na utrzymującą się dużą liczbę wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych zgłoszeń zbiorów danych nadsyłanych do rejestracji przez centralne organy administracji rządowej, a zwłaszcza ministrów kierujących określonymi działami administracji rządowej. Zgłoszenia te niejednokrotnie dotyczyły przetwarzania danych osobowych w centralnych bazach lub zintegrowanych systemach informatycznych. Tytułem przykładu można wskazać następujące zbiory danych: „SYSTEM POWIADAMIANIA RATUNKOWEGO" i „PORTAL ZBIÓREK PUBLICZNYCH" zgłoszony do rejestracji przez Ministra Administracji i Cyfryzacji, czy „ZINTEGROWANY SYSTEM ZARZĄDZANIA RYZYKIEM ZISAR" zgłoszony do rejestracji przez Ministra Finansów. W przypadku tego typu zbiorów często konieczne jest przeprowadzenie postępowania wyjaśniającego, a przekazywanie wiedzy z zakresu ochrony danych osobowych okazuje się niezbędne nawet w przypadku tego rodzaju podmiotów. Charakterystycznym przykładem są zbiory zgłoszone do rejestracji przez Ministra Sprawiedliwości. Tylko w dwóch przypadkach treść zgłoszenia nie budziła zastrzeżeń i

umożliwiała wpisanie zbioru do ogólnokrajowego, jawnego rejestru zbiorów danych osobowych według pierwotnych informacji. W przypadku pozostałych zgłoszeń niezbędne było przeprowadzenie złożonych postępowań wyjaśniających. Ich pozytywne wyniki umożliwiły wpisanie zgłoszonych zbiorów do rejestru zbiorów danych osobowych. Ponadto kolejne wpływające do Departamentu Rejestracji Zborów Danych Osobowych zgłoszenia rejestracyjne pochodzące od Ministra Sprawiedliwości, wypełniane są z dużo większą starannością, co pozwala przyjąć, iż przekazana wiedza z zakresu ochrony danych osobowych została właściwie wykorzystana.

Najczęściej powtarzającym się problemem było niewłaściwe określenie podstawy prawnej upoważniającej organ państwowy do przetwarzania danych w prowadzonym zbiorze. W przypadku podmiotów publicznych uprawnienie bądź obowiązek wykonania określonych zadań i związana z tym konieczność gromadzenia danych o osobach, powinna wynikać z przepisu kompetencyjnego. Administratorzy informowali zaś często w treści zgłoszeń, że podstawę legalizującą przetwarzanie danych stanowi zgoda osoby, której dane dotyczą.

Zgłoszenia nadsyłane przez organy państwowe i samorządowe, ale także podmioty prywatne, dotyczą nieraz więcej niż jednego zbioru danych. Wypełnienie jednego zgłoszenia dla kilku zbiorów danych osobowych nie pozwala w sposób właściwy scharakteryzować poszczególnych zbiorów objętych tym zgłoszeniem, tym samym nie można dla każdego z nich wskazać elementów decydujących o jego tożsamości, tj. np. zakresu przetwarzanych danych, celu przetwarzania danych w zbiorze, a co za tym idzie nie jest możliwe stwierdzenie, jaki zakres informacji objętych zgłoszeniem dotyczy każdego ze zbiorów. W związku z tym administrator jest w takim przypadku informowany o konieczności zgłoszenia każdego zbioru na odrębnym formularzu.

W postępowaniach rejestracyjnych dotyczących zbiorów zgłaszanych przez organy centralne często wymaga wyjaśnienia status podmiotów biorących udział w procesie przetwarzania danych. Administratorzy informują bowiem o zawarciu umowy powierzenia przetwarzania danych osobowych z podmiotem zapewniającym techniczno-informatyczną obsługę prowadzonych przez nich zbiorów danych. W toku postępowań okazuje się często, że do powierzenia przetwarzania danych w rzeczywistości nie dochodzi. Przykładowo przepisy ustawy z dnia 14 marca 2014 r. o zasadach prowadzenia zbiórek publicznych (Dz. U. z 2014 r. poz. 498) nałożyły na ministra właściwego do spraw administracji publicznej (Ministra Administracji i Cyfryzacji) obowiązek prowadzenia ogólnopolskiego portalu zbiórek publicznych. Zgodnie z art. 5 ust. 1 ww. ustawy zbiórka publiczna może zostać

przeprowadzona po jej zgłoszeniu przez organizatora zbiórki i zamieszczeniu informacji o zgłoszeniu przez ministra właściwego do spraw administracji publicznej na ogólnopolskim elektronicznym portalu zbiórek publicznych. W związku z powołanymi przepisami Minister Administracji i Cyfryzacji zgłosił do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych osobowych o nazwie „PORTAL ZBIÓREK PUBLICZNYCH". W pkt 3 części B zgłoszenia administrator danych wskazał Centrum Projektów Informatycznych, jako podmiot, któremu powierzył w drodze umowy, o której mowa w art. 31 ustawy, przetwarzanie danych zawartych w przedmiotowym zbiorze. Zgodnie ze statutem Centrum Projektów Informatycznych, Centrum jest jednostką budżetową podległą Ministrowi Administracji i Cyfryzacji. Ponadto, stosownie do § 2 ust. 1 pkt 1 statutu, Centrum realizuje zadania w zakresie informatyzacji i teleinformatyki powierzone, w drodze decyzji, przez Ministra Administracji i Cyfryzacji i pozostające w jego właściwości. W toku postępowania rejestracyjnego Departament Rejestracji Zborów Danych Osobowych wyjaśnił, iż w przedmiotowej sprawie nie doszło do powierzenia przetwarzania danych w trybie art. 31 ustawy, bowiem zakres i cel przetwarzania danych przez Centrum Projektów Informatycznych został określony (powierzony) w decyzji Ministra Administracji i Cyfryzacji. W świetle powyższego przedmiotowy zbiór został wpisany do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych ogólnokrajowego, jawnego rejestru zbiorów danych osobowych.

Podobna sytuacja miała miejsce w przypadku Ministra Spraw Wewnętrznych, który w związku z realizacją obowiązków wynikających z przepisów ustawy z dnia 9 listopada 2000 r. o repatriacji (Dz. U. z 2004 r. Nr 53, poz. 532 z późn. zm.) oraz ustawy z dnia 2 kwietnia 2009 r. o obywatelstwie polskim (Dz. U. z 2012 r. poz. 161 z późn. zm.), zgłosił do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiory danych osobowych o nazwach „REPATRIANT" i „OBYWATELSTWO". W treści ww. zgłoszeń wnioskodawca wskazał Szefa Urzędu do Spraw Cudzoziemców jako podmiot, któremu administrator danych, tj. Minister Spraw Wewnętrznych powierzył w drodze umowy, o której mowa w art. 31 ustawy o ochronie danych osobowych, przetwarzanie danych zawartych w przedmiotowych zbiorach. W związku z tym, iż zadania związane z przetwarzaniem danych osobowych w ww. zbiorach danych realizowane są zarówno przez Ministra Spraw Wewnętrznych jak i Szefa Urzędu do Spraw Cudzoziemców i wynikają z obowiązujących przepisów prawa, Departament Rejestracji Zborów Danych Osobowych zwrócił uwagę, że zbędne wydaje się nadanie przez Ministra Spraw Wewnętrznych upoważnienia Szefowi Urzędu do Spraw

Cudzoziemców „do przetwarzania danych". Brak jest też podstaw by twierdzić, że na podstawie tego upoważnienia doszło do powierzenia przetwarzania danych, o którym mowa w art. 31 ustawy o ochronie danych osobowych. Administrator danych zgodził się ze stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych. Dodatkowo Szef Urzędu do Spraw Cudzoziemców wystąpił z wnioskiem o wykreślenie z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych zbioru danych osobowych o nazwie „CENTRALNY REJESTR O NABYCIU I UTRACIE OBYWATELSTWA POLSKIEGO" – nadesłanego do rejestracji przez Prezesa Urzędu do Spraw Repatriacji i Cudzoziemców (obecnie Szef Urzędu do Spraw Cudzoziemców) w związku z tym, że obecnie, zgodnie z ustawą o obywatelstwie polskim, minister właściwy do spraw wewnętrznych tworzy i prowadzi w systemie teleinformatycznym centralny rejestr danych o nabyciu i utracie obywatelstwa polskiego i w myśl art. 59 ust. 2 ustawy o obywatelstwie jest administratorem danych przetwarzanych w tym rejestrze. Mając na uwadze powołane uregulowania prawne oraz zgłoszenie przez Ministra Spraw Wewnętrznych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych o nazwie "OBYWATELSTWO" prowadzonego na podstawie art. 59 ustawy o obywatelstwie polskim, zbiór danych o nazwie „CENTRALNY REJESTR O NABYCIU I UTRACIE OBYWATELSTWA POLSKIEGO" został wykreślony z rejestru zbiorów danych osobowych.

Wejście w życie nowych przepisów prawnych skutkuje zgłaszaniem do rejestracji przez administratorów danych osobowych nowych zbiorów tworzonych w związku z realizacją zadań lub kompetencji wynikających z wprowadzanych regulacji. Zgodnie z art. 5c ust. 1 i 5d ustawy z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz. U. z 2012 r. poz. 1059 z późn. zm.), które dodane zostały na skutek wejścia w życie ustawy z dnia 26 lipca 2013 r. o zmianie ustawy - Prawo energetyczne oraz niektórych innych ustaw (Dz. U. z 2013 r. poz. 984), odbiorcy wrażliwemu energii elektrycznej przysługuje zryczałtowany dodatek energetyczny. Dodatek przyznaje wójt, burmistrz lub prezydent miasta, w drodze decyzji, na wniosek odbiorcy wrażliwego energii elektrycznej. Zbiory danych osobowych związane z przyznawaniem ww. dodatków zgłaszają do rejestracji gminy, ale również ośrodki pomocy społecznej. Uzasadniając zgłoszenie ww. zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych ośrodki pomocy społecznej powołują zapisy 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 do załatwiania indywidualnych spraw z zakresu administracji

publicznej rada gminy może upoważnić również organ wykonawczy jednostki pomocniczej oraz organy jednostek i podmiotów utworzonych przez gminę w celu wykonywania zadań gminy lub podmiotów, z którymi gmina zawarła odpowiednie umowy. W wyniku przeprowadzonych postępowań wyjaśniających ustalono, że w przypadku upoważnienia kierownika ośrodka pomocy społecznej do załatwiania indywidualnych spraw w zakresie przyznawania dodatków energetycznych ośrodkowi przysługuje status administratora danych osób ubiegających się o przyznanie dodatku i osób taki dodatek otrzymujących. Dodać należy, że zarówno gminy jak i ośrodki pomocy społecznej zgłaszają do rejestracji zbiory danych dotyczące przyznawania dodatków energetycznych odrębnie jako nowe zbiory albo zgłaszają odpowiednie aktualizacje zbiorów danych prowadzonych w związku z przyznawaniem dodatków mieszkaniowych. Biorąc pod uwagę, że odbiorca wrażliwy energii elektrycznej to zgodnie z definicją legalną osoba, której przyznano dodatek mieszkaniowy w rozumieniu art. 2 ust. 1 ustawy z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych (Dz. U. z 2013 r. poz. 966 z późn. zm.), która jest stroną umowy kompleksowej lub umowy sprzedaży energii elektrycznej zawartej z przedsiębiorstwem energetycznym i zamieszkuje w miejscu dostarczania energii elektrycznej (art. 3 pkt 13c Prawa energetycznego), istnieje ścisły związek między przyznaniem dodatku mieszkaniowego i energetycznego. W konsekwencji należało uznać, że dopuszczalne jest również zgłoszenie ww. zmian w zbiorach danych dotyczących przyznawania dodatków mieszkaniowych.

W dniu 15 maja 2014 r. weszła w życie ustawa z dnia 4 kwietnia 2014 r. o ustaleniu i wypłacie zasiłków dla opiekunów (Dz.U. z 2014 r. poz. 567), określająca warunki nabywania oraz zasady ustalania i wypłacania zasiłków dla opiekunów osobom, które utraciły prawo do świadczenia pielęgnacyjnego z dniem 1 lipca 2013 r. w związku z wygaśnięciem z mocy prawa decyzji przyznającej prawo do świadczenia pielęgnacyjnego. Zgodnie z art. 5 ust. 1 ww. ustawy postępowanie w sprawie ustalenia prawa do zasiłku dla opiekuna organ ustalający prawo do świadczeń pielęgnacyjnych wszczyna na wniosek osoby ubiegającej się o zasiłek dla opiekuna. Realizacja zasiłków dla opiekunów jest zadaniem zleconym z zakresu administracji rządowej realizowanym przez gminy, a w sprawach nieuregulowanych w ustawie stosuje się odpowiednio przepisy ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz. U. z 2013 r. poz. 1456, z późn. zm.) dotyczące świadczeń pielęgnacyjnych (art. 9 ust. 2 i 10 ust. 1 ustawy o ustaleniu i wypłacie zasiłków dla opiekunów). Zbiory danych związane z przyznawaniem zasiłków dla opiekunów zgłaszane są przez gminy, a w przypadku upoważnienia kierownika ośrodka pomocy społecznej do prowadzenia postępowania w

sprawie świadczeń rodzinnych i utworzenia w ośrodku komórki organizacyjnej do realizacji tych świadczeń, zgodnie z art. 20 ust. 3 i 4 ustawy o świadczeniach rodzinnych, ośrodki pomocy społecznej.

Zgłaszane do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych były również zbiory danych prowadzone na podstawie przepisów rozporządzenia Rady Ministrów z dnia 27 maja 2014 r. w sprawie szczegółowych warunków realizacji rządowego programu dla rodzin wielodzietnych (Dz. U. z 2014 r. poz. 755). Powołane przepisy uregulowały realizację w gminach rządowego programu dla rodzin wielodzietnych. Zgodnie z § 20 ust. 2 ww. rozporządzenia administratorami danych osobowych przetwarzanych w zakresie niezbędnym do przyznawania karty dużej rodziny oraz wydawania jej duplikatu są wójt oraz minister właściwy do spraw zabezpieczenia społecznego i w związku z tym powyższe podmioty zobowiązane są do zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

W związku z powołanymi przepisami Minister Pracy i Polityki Społecznej zgłosił do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „KARTA DUŻEJ RODZINY" – zgłoszenie nr R 018879/14. Również wiele gmin zgłosiło zbiory danych osobowych dotyczących przyznawanych kart. Jednakże w części zgłoszeń dotyczących realizacji tych zadań jako administratorzy danych wskazane zostały ośrodki pomocy społecznej. Dlatego też, w świetle jednoznacznych zapisów ww. rozporządzenia, do ośrodków pomocy społecznej kierowane były pisma z informacją, iż nie są one administratorami danych przetwarzanych w zgłaszanych do rejestracji zbiorach prowadzonych w związku z realizacją w gminach rządowego programu dla rodzin wielodzietnych.

Warto dodać, że w gminach realizowane są również, w oparciu o przepisy ustawy z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2013 r. poz. 182 z późn. zm.), gminne programy działań promujących rodziny wielodzietne (np. karty rodziny 3+ lub 4+) zamieszkałe na terenie danej gminy. Zasady realizacji tych programów, zmierzających do polepszenia warunków życiowych rodzin wielodzietnych, określane są w drodze uchwały rady gminy. Realizacja tego zadania często powierzana jest ośrodkom pomocy społecznej. Uznać należy, że w takim przypadku ośrodek jest administratorem danych przetwarzanych w związku z realizacją gminnej pomocy dla rodzin wielodzietnych. Nową kategorię zbiorów zgłaszanych przez gminy i ośrodki pomocy społecznej stanowiły również zbiory prowadzone w związku z weryfikacją oświadczeń składanych w toku rekrutacji prowadzonej przez

jednostki oświatowe, zgodnie z nowymi przepisami wprowadzonymi ustawą z dnia 6 grudnia 2013 r. o zmianie ustawy o systemie oświaty oraz niektórych innych ustaw (Dz. U. z 2014 r. poz. 7). W wyniku wskazanej nowelizacji w ustawie o systemie oświaty dodany został rozdział 2a Przyjmowanie do publicznych przedszkoli, publicznych innych form wychowania przedszkolnego, publicznych szkół i publicznych placówek. Nowe przepisy określają m.in. jakie elementy powinien zawierać wniosek o przyjęcie do placówki oraz wykaz dokumentów, w tym oświadczeń, jakie do wniosku należy załączyć. Jednocześnie w art. 20t ust. 7 – 10 ustawy o systemie oświaty określano zasady weryfikacji okoliczności zawartych w oświadczeniach składanych w toku rekrutacji do placówki oświatowej. Zgodnie z ww. przepisami przewodniczący komisji rekrutacyjnej może m.in. zwrócić się do wójta (burmistrza, prezydenta miasta) właściwego ze względu na miejsce zamieszkania kandydata o potwierdzenie tych okoliczności. W celu potwierdzenia okoliczności zawartych w oświadczeniach, wójt (burmistrz, prezydent miasta) właściwy ze względu na miejsce zamieszkania kandydata korzysta z informacji, które zna z urzędu, lub może wystąpić do instytucji publicznych o udzielenie informacji o okolicznościach zawartych w oświadczeniach, jeżeli instytucje te posiadają takie informacje. Oświadczenie o samotnym wychowywaniu dziecka może być zweryfikowane w drodze wywiadu, o którym mowa w art. 23 ust. 4a ustawy o świadczeniach rodzinnych. Do prowadzenia spraw, o których mowa wyżej wójt (burmistrz, prezydent miasta) właściwy ze względu na miejsce zamieszkania kandydata może upoważnić kierownika ośrodka pomocy społecznej, kierownika innej jednostki organizacyjnej gminy lub inną osobę na wniosek kierownika ośrodka pomocy społecznej, lub kierownika innej jednostki organizacyjnej gminy.

W omawianym okresie weszły również w życie przepisy ustawy z dnia 23 października 2013 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw (Dz. U. z 2013 r. poz. 1446). Wynikiem tej nowelizacji były zgłoszenia do rejestracji składane przez administratorów danych osobowych nowych zbiorów tworzonych w związku z realizacją zadań w zakresie wydawania kart parkingowych dla osób niepełnosprawnych kierujących pojazdem samochodowym, które mogą nie stosować się do niektórych znaków drogowych. W dotychczasowym stanie prawnym kompetencje w tym zakresie posiadał starosta, a do ogólnokrajowego rejestru wpisywane były zbiory danych związane z realizacją tych zadań zgłaszane przez powiaty. Obecnie karty parkingowe dla osób niepełnosprawnych wydaje przewodniczący powiatowego zespołu do spraw orzekania o niepełnosprawności na podstawie orzeczenia wydanego przez zespół do spraw orzekania o niepełnosprawności. W

konsekwencji do rejestru wpisywane są zbiory dotyczące wydawania tych kart, których administratorami są powiatowe zespoły. Na powiatach ciąży natomiast obowiązek zgłoszenia zmian w zbiorach, które zgłosiły one pod rządami zmienionych przepisów, w tym zawiadomienia o zaprzestaniu przetwarzania danych w takich zbiorach.

Wśród zgłoszeń do rejestracji pochodzących od podmiotów publicznych, w dalszym ciągu stosunkowo dużą liczbę stanowiły składane przez gminy zgłoszenia zbiorów danych osobowych prowadzonych 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.). Większość zbiorów została zgłoszona do rejestracji w związku z nowelizacją ww. ustawy dokonaną 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). 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 pomocą deklaracji. Określając, w drodze uchwały, wzór deklaracji rada gminy wskazała w konsekwencji także zakres danych osobowych pozyskiwanych przez gminę za jej pomocą.

Wątpliwości budził nieraz zakres pozyskiwanych danych o właścicielach nieruchomości, dlatego konieczne było przeprowadzenie postępowań wyjaśniających dotyczących zakresu danych zawartych w deklaracjach. Odpowiadając na wezwania do złożenia wyjaśnień administratorzy danych w większości przypadków informowali o ograniczeniu zakresu pozyskiwanych do zbioru danych osobowych. Niekiedy jednak wskazywali, że zgłoszony do rejestracji zbiór obejmuje nie tylko deklaracje o wysokości opłaty za odpady, ale również dane przetwarzane w związku z naliczaniem, pobieraniem oraz egzekucją opłat. W takich przypadkach Generalny Inspektor Ochrony Danych Osobowych, działając na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych, zwracał się do organów stanowiących i kontrolnych (rad gmin, rad miejskich, zgromadzenia związku międzygminnego) o podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanych przez właścicieli nieruchomości, w zakresie zapewnienia zgodności wzorów deklaracji z przepisami o ochronie danych osobowych. Pozytywne odpowiedzi na wystąpienia dały podstawę do wpisania przedmiotowych zbiorów do rejestru zbiorów danych osobowych.

W 2014 r. GIODO wystąpił do Podsekretarza Stanu w Ministerstwie Pracy i Polityki Społecznej - Krajowego Koordynatora Realizacji Krajowego Programu Przeciwdziałania

Przemocy w Rodzinie oraz przewodniczącej Zespołu Monitorującego do spraw Przeciwdziałania Przemocy w Rodzinie, w sprawie podstawy prawnej przetwarzania danych osobowych szczególnie chronionych przez członków zespołów interdyscyplinarnych.

W związku z realizacją zadań w zakresie przeciwdziałania przemocy w rodzinie oraz prowadzeniem postępowań wobec osób dotkniętych przemocą w rodzinie i stosujących przemoc, zespoły interdyscyplinarne pozyskują bardzo szeroki zakres danych osobowych, w tym dane szczególnie chronione. Zgodnie z art. 9c ust. 1 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie (Dz. U. z 2005 r. Nr 180 poz. 1493 z późn. zm.) członkowie zespołu interdyscyplinarnego oraz grup roboczych w zakresie niezbędnym do realizacji swoich zadań mogą przetwarzać dane osób dotkniętych przemocą w rodzinie i osób stosujących przemoc w rodzinie, dotyczące: stanu zdrowia, nałogów, skazań, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, bez zgody i wiedzy osób, których dane te dotyczą.

Zbiory obejmujące dane zebrane w wyniku działalności zespołów interdyscyplinarnych podlegają obowiązkowi zgłoszenia do rejestracji. W treści składanych w Biurze Generalnego Inspektora Ochrony Danych Osobowych zgłoszeń dotyczących ww. zbiorów niejednokrotnie administratorzy danych (ośrodki pomocy społecznej, które zapewniają obsługę organizacyjno-techniczną ww. zespołów) wskazują, że oprócz danych określonych w art. 9c ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie, do ww. zbiorów pozyskiwane są również inne kategorie danych szczególnie chronionych, w tym zwłaszcza dane ujawniających pochodzenie rasowe lub etniczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, jak również dane o życiu seksualnym, czy dane dotyczące mandatów karnych. Administratorzy danych uzasadniali pozyskiwanie ww. danych m.in.:

- przydatnością informacji o przynależności wyznaniowej i przekonaniach religijnych w obszarze motywacji sprawców przemocy do pracy nad sobą i zmiany zachowań - oddziaływania korekcyjno-edukacyjne (art. 4 ustawy o przeciwdziałaniu przemocy w rodzinie),
- występowaniem przemocy na tle religijnym, wyznaniowym, etnicznym i rasowym w rodzinach, których członkowie są różnych wyznań, narodowości, itd.,
- obecnością na obszarze działania zespołu licznej grupy rodzin romskich i występowaniem przemocy w tym środowisku związanej z pochodzeniem etnicznym np. przyzwoleniem na związki osób nieletnich,

- zapewnieniem prawa do wolności religijnej w kontekście udziału w pracy grup roboczych przedstawicieli wspólnot religijnych lub związków wyznaniowych - współpraca z kościołami i związkami wyznaniowymi (art. 9 ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie),
- występowaniem przemocy na tle seksualnym - naruszenie wolności seksualnej wskazane zostało w definicji przemocy w rodzinie (art. 2 pkt 2 ustawy o przeciwdziałaniu przemocy w rodzinie),
- koniecznością rozpoznania sytuacji w celu udzielenia wsparcia socjalno-psychologicznego ofiarom przemocy, opracowania planu pomocy tym osobom.

Administratorzy często deklarują przy tym, że ww. dane pojawiają się w toku prowadzonych i protokołowanych rozmów np. gdy osoba uzasadnia swoje czyny wyznaniem. Mogą zostać także pozyskane w ramach procedury „Niebieska Karta" - jako przyczyna przemocy lub w opisie zdarzenia „przemocowego".

W kontekście składanych w toku postępowania rejestracyjnego wyjaśnień nie sposób przyjąć, że pozyskiwane przez zespoły interdyscyplinarne w toku ich działań dane szczególnie chronione wykraczające poza katalog wskazany w art. 9c ust. 1 ustawy są zbędne dla realizacji zadań tych zespołów. W wielu przypadkach można wręcz uznać, że posiadanie tych informacji decyduje o skuteczności podejmowanych działań lub wręcz warunkuje możliwość ich podjęcia. Trudno wobec tego dopatrywać się tu naruszenia zasady adekwatności tj. pozyskiwania danych nieuzasadnionych celem ich przetwarzania.

Podkreślić jednak należy, że w toku postępowania rejestracyjnego Generalny Inspektor Ochrony Danych Osobowych badał również, czy w konkretnym przypadku występowała przesłanka legalizująca przetwarzanie danych osobowych, w tym danych szczególnie chronionych. Trzeba bowiem pamiętać, że przetwarzanie tego rodzaju danych jest co do zasady zakazane, a wyjątki od tego zakazu zostały enumeratywnie wymienione w art. 27 ust. 2 ustawy o ochronie danych osobowych. Dla podmiotów publicznych podstawowe znaczenie ma przesłanka przetwarzania danych szczególnie chronionych określona w art. 27 ust. 2 pkt 2 ustawy, tj. przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony. Takim przepisem szczególnym jest, przytoczony wyżej, art. 9c ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie.

Istotne problemy wiążą się natomiast z wykazaniem istnienia podstawy prawnej do przetwarzania danych szczególnie chronionych innych niż określone w ww. przepisie.

Niektóre ośrodki pomocy społecznej informują w treści zgłoszeń lub składanych w toku postępowania wyjaśnieniach, że uzyskują pisemną zgodę na przetwarzanie danych od osób, których te dane dotyczą, a więc spełniona jest przesłanka wynikająca z art. 27 ust. 2 pkt 1 ustawy. Jednakże większość ośrodków powołuje się wyłącznie na przepisy ustawy o przeciwdziałaniu przemocy w rodzinie i rozporządzenia Rady Ministrów z dnia 13 września 2011 r. w sprawie procedury „Niebieskie Karty" oraz wzorów formularzy „Niebieska Karta" (Dz. U. z 2011 r. Nr 209 poz. 1245). Niektóre z nich wskazują przy tym, że nie można przyjąć np., że sprawcy przemocy będą dobrowolnie wyrażać na piśmie zgodę na przetwarzanie dotyczących ich danych szczególnie chronionych innych niż wynikające z art. 9c ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie.

W kontekście jednoznacznego brzmienia ww. przepisu (który odbiega w tym względzie od rozwiązań przyjętych w innych ustawach mających na celu udzielanie pomocy rodzinom jak np. art. 29 ust. 1 ustawy o świadczeniach rodzinnych lub art. 7 ustawy o wspieraniu rodziny i systemie pieczy zastępczej) trudno jest uznać, że przepisy ustawy o przeciwdziałaniu przemocy w rodzinie stanowią podstawę do pozyskiwania np. informacji ujawniających pochodzenie rasowe lub etniczne, przekonania religijne lub filozoficzne czy przynależność wyznaniową. Co więcej zamknięty katalog danych z art. 9c ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie wydaje się nie uwzględniać kategorii danych wynikających z innych przepisów tej ustawy oraz wzorów formularzy „Niebieska Karta". Wskazać tu należy chociażby na pojecie naruszenia wolności seksualnej zawarte w ustawowej definicji przemocy oraz informacje o stosowaniu przemocy seksualnej zawarte w pkt IV części A i pkt II części D „Niebieskiej Karty". Innym przykładem jest obowiązek współdziałania z kościołami i związkami wyznaniowymi m.in. w zakresie udzielania pomocy osobom dotkniętym przemocą i oddziaływania na osoby stosujące przemoc, gdzie przekonania religijne i przynależność wyznaniowa ofiary przemocy lub jej sprawcy może mieć kluczowe znaczenie dla podjęcia wspólnych działań w stosunku do danej osoby. Zaznaczyć należy również, że katalog z art. 9c ustawy o przeciwdziałaniu przemocy w rodzinie jest węższy niż katalog danych wrażliwych wskazany w art. 100 ustawy o pomocy społecznej, mimo że zgodnie z art. 6 ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie zadania w zakresie przeciwdziałania przemocy w rodzinie są realizowane m.in. na zasadach określonych w ustawie o pomocy społecznej, a przedstawiciele jednostek organizacyjnych pomocy społecznej wchodzą w skałd zespołu interdyscyplinarnego i grup roboczych, wykonując zadania w ramach obowiązków służbowych lub zawodowych (art. 9a ust. 3, 11 i

13 ww. ustawy).

Podkreślenia wymaga, że rozporządzenie w sprawie procedury „Niebieskie Karty" oraz wzorów formularzy „Niebieska Karta", jako akt rangi niższej niż ustawa, nie może stanowić podstawy pozyskiwania danych szczególnie chronionych.

Biorąc powyższe pod uwagę oraz uwzględniając doniosłość zadań realizowanych przez zespoły interdyscyplinarne, a także znaczenie ich działań w zakresie przeciwdziałania przemocy w rodzinie dla zagwarantowania podstawowych praw człowieka, w tym prawa do życia, zdrowia i poszanowania godności osobistej, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Krajowego Koordynatora Realizacji Krajowego Programu Przeciwdziałania Przemocy w Rodzinie o rozważenie podjęcia działań legislacyjnych, w celu rozwiązania opisanego wyżej problemu dotyczącego podstawy prawnej do pozyskiwania w toku pracy zespołów interdyscyplinarnych danych szczególnie chronionych.

W związku z wejściem z życie w dniu 11 maja 2014 r. nowelizacji Kodeksu postępowania administracyjnego oraz ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, dokonanych ustawą z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2014 r., poz. 183), GIODO podjął szereg działań mających na celu przygotowanie się do realizacji nowych zasad doręczania w formie elektronicznej pism w prowadzonych postępowaniach.

W dotychczasowym stanie prawnym doręczenia były realizowane w formie elektronicznej jeśli strona wystąpiła o to do organu administracji publicznej lub wyraziła zgodę na doręczenie jej pism w ww. formie. Zgodnie z przepisami obowiązującymi od 11 maja 2014 r., w przypadku złożenia przez stronę podania w formie dokumentu elektronicznego przez elektroniczną skrzynkę podawczą organu administracji publicznej, doręczanie jej pism w toku postępowania następuje za pomocą środków komunikacji elektronicznej. Strona ma prawo do rezygnacji z doręczeń drogą elektroniczną, ale w razie braku stosowanego oświadczenia strony w tym względzie, doręczenia powinny być dokonywane w tej formie. Wprowadzono również rozwiązanie, zgodnie z którym w razie nieodebrania pisma przesłanego w formie elektronicznej, pismo to nie będzie już wysyłane w formie tradycyjnej. Po dwukrotnym zawiadomieniu, jeśli strona nie odbierze pisma, uznaje się je bowiem za doręczone po upływie 14 dni od pierwszego zawiadomienia o możliwości odebrania pisma przesłanego drogą elektroniczną.

Dostosowanie się do nowych zasad dokonywania doręczeń w toku prowadzonych przez

GIODO spraw wymagało wprowadzenia nowych rozwiązań na platformie e-GIODO. W zakresie funkcjonowania programu służącego do wypełniania wniosku o rejestrację zbioru danych osobowych wprowadzono nowe pole wyboru (check box) z oświadczeniem o rezygnacji z doręczeń w drodze elektronicznej. Jest to rozwiązanie uniwersalne wprowadzone również dla innej korespondencji kierowanej do Biura Generalnego Inspektora Ochrony Danych Osobowych przez elektroniczną skrzynkę podawczą. Zostało ono również przewidziane przez Ministra Administracji i Cyfryzacji dla systemu ePUAP. Kolejna modyfikacja dotyczyła zablokowania na platformie e-GIODO opcji wysłania wniosku bez podpisu elektronicznego, gdy strona nie odznaczyła *check boxu* rezygnacji z doręczeń elektronicznych. Po wypełnieniu wniosku pole wysyłania jest dla niepodpisanych zgłoszeń aktywne tylko w razie rezygnacji z doręczeń elektronicznych. Również w przypadku wczytania wniosku wcześniej zapisanego można będzie go wysłać tylko, gdy zostanie podpisany lub gdy przy wypełnianiu strona zrezygnuje z doręczeń elektronicznych. Pozwala to wyeliminować wysyłanie przez Generalnego Inspektora Ochrony Danych Osobowych pism drogą elektroniczną do osób nie mogących ich odebrać. Jednocześnie zostały umieszczone odpowiednie komunikaty informujące, że w razie braku podpisu elektronicznego weryfikowanego certyfikatem kwalifikowanym lub profilu zaufanego ePUAP należy zrezygnować z doręczeń elektronicznych.

Nowe zasady doręczeń elektronicznych dotyczą spraw wszczętych od dnia wejścia w życie nowelizacji. W praktyce oznacza to, że w przypadku wpłynięcia przez platformę e-GIODO podpisanego elektronicznie zgłoszenia, gdy strona nie zrezygnowała z doręczeń elektronicznych, wszelką korespondencję do niej kieruje się wyłącznie w tej formie. W zależności od tego, czy zgłoszenie zostanie przesłane przez ePUAP, czy też podpisane certyfikatem kwalifikowanym, korespondencja do strony wysyłana jest przy użyciu platformy ePUAP albo systemu Doręczyciel.

Znaczenie opisanych zmian dla pracy Biura GIODO obrazuje statystyka – w roku 2014 wpłynęło do 32 720 zgłoszeń przesłanych za pośrednictwem platformy e-GIODO. Do tego doliczyć należy zgłoszenia aktualizacyjne i wydawane zaświadczenia o zarejestrowaniu zbioru danych osobowych.

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 2014 roku do grona szkół wyższych, z którymi GIODO zawarł porozumienia o współpracy, dołączył Uniwersytet Jagielloński oraz Społeczna Akademią Nauk z siedzibą w Łodzi.

Generalny Inspektor Ochrony Danych Osobowych od wielu lat aktywne współpracuje z różnymi podmiotami w obszarze przestrzegania zasad ochrony danych osobowych. Wśród nich wymienić można np. Najwyższą Izbę Kontroli czy Państwową Inspekcję Pracy. W oparciu o informacje przekazywane Generalnemu Inspektorowi przez te podmioty podejmowane są działania mające na celu uczulenie kontrolowane podmioty na obowiązek stosowania przepisów ustawy o ochronie danych osobowych w prowadzonej przez nie działalności.

Wspomnieć także należy, że podczas 94. posiedzenia Grupy Roboczej Art. 29 (26-27.02.2014) odpowiadając na pytania kwestionariusza dotyczącego roli i zadań polskiego organu ds. ochrony danych osobowych, przedstawił prezentację z przebiegu współpracy GIODO z Najwyższą Izbą Kontroli oraz Państwową Inspekcją Pracy w sprawie prowadzenia wspólnych inspekcji i wymiany doświadczeń.

Postępujący proces transformacji ze społeczeństwa informacyjnego w społeczeństwo sieciowe i związana z nim cyfryzacja, wywołuje obawy o zatrudnienie, ochronę prywatności i danych osobowych. Ale z drugiej strony coraz wyraźniej widać, jak wzrost gospodarczy napędzany siłą Internetu tworzy potencjał rozwojowy państwa i społeczeństwa. Dostrzegając wagę tego procesu Generalny Inspektor Ochrony Danych Osobowych angażuje się w działania w zakresie podnoszenia świadomości obywateli w kwestii zarządzania prywatnością w sieci, budowaniu zaufania i zachęcania do korzystania z udogodnień gospodarki cyfrowej.

Jest członkiem **Partnerstwa dla zwiększenia świadomości i wiedzy obywateli na temat cyfrowej tożsamości**, którego misją jest zwiększanie wiedzy obywateli o sposobach zarządzania prywatnością w sieci i świadomym – opartym na przejrzystych zasadach – wykorzystaniu cyfrowej tożsamości w celu rozwoju gospodarki internetowej oraz 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.

Przedmiotem szczególnej uwagi GIODO są **aplikacje mobilne** i zagadnienie spełniania standardów dotyczących ochrony prywatności i danych osobowych przy ich tworzeniu, jako warunku zapewniającego ich bezpieczne użytkowanie. Zaniepokojenie bowiem budzą wyniki badań[476] ponad 1200 aplikacji mobilnych przeprowadzonych przez Światową Sieć Egzekwowania Przepisów o Ochronie Prywatności (GPEN)[477]. Wynika z nich, że 85 % pośród badanych aplikacji mobilnych wymaga od użytkownika podania danych osobowych bez informowania w odpowiedni sposób, jak informacje te będą wykorzystywane, a ponad połowa (59 %) przedstawiała informację o ochronie prywatności w trudny do odnalezienia sposób.

W tym miejscu podkreślenia wymaga, że aplikacje mobilne, w tym coraz powszechniejsze urządzenia monitorujące styl życia, mogą gromadzić różne dane osobowe, w tym również dane o stanie zdrowia, które podlegają szczególnej ochronie. Nierzadko bowiem producenci aplikacji nie do końca zdają sobie sprawę, że ich wyroby mogą być jednocześnie urządzeniami medycznymi, rejestrującymi dane biometryczne użytkownika. Nawet technologie komunikacji bezprzewodowej (RFID) powszechnie instalowane w różnych urządzeniach, z pozoru niemających związku z przetwarzaniem danych o stanie zdrowia, umożliwiają gromadzenie i wymianę danych medycznych o użytkowniku. Bo na przykład poprzez WI-FI możliwa już będzie identyfikacja lokalizacji użytkowników i wyciąganie wniosków na temat ich zachowań, które w szczególnych przypadkach mogą być związane ze stanem zdrowia (np. pobyt w szpitalu). Aplikacje są więc tak zaprojektowane, aby zbierać dane osobowe i w praktyce często przetwarzają dane o stanie zdrowia. Technologie takie jak

[476] https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp

[477] Od listopada 2010 r. GIODO jest oficjalnym członkiem Światowej Sieci Egzekwowania Przepisów o Ochronie Prywatności (Global Privacy Enforcement Network – GPEN); zob. też: http://www.giodo.gov.pl/1520099/j/pl/

ekran wielodotykowy, przyspieszeniomierze lub żyroskopy, czujniki natężenia oświetlenia, GPS, kamery, aparaty fotograficzne oraz urządzenia posiadające czytniki linii papilarnych i czytniki biometryczne wiążą się z gromadzeniem danych medycznych. Nawet aplikacja telefonu komórkowego może monitorować dane fizjologiczne użytkownika, takie jak bicie serca, wzorce snu, czy informacje dotyczące sprawności fizycznej.

Na problematykę aplikacji mobilnych zwrócili uwagę rzecznicy ochrony danych osobowych podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności – *Prywatność: Przewodnik po zagmatwanym świecie* (2013 r.), przyjmując **„Deklarację Warszawską w sprawie upowszechniania się aplikacji mobilnych"**, w której zachęcają do globalnego wysiłku na rzecz zapewnienia pełnej kontroli użytkownika nad dotyczącymi go danymi osobowymi. Rzecznicy ochrony danych osobowych na całym świecie zamierzają zintensyfikować działania na rzecz poprawy ochrony danych i prywatności w tym obszarze, zwracając się do wszystkich interesariuszy zarówno w sektorze publicznym, jak i prywatnym, w związku z ich rolą i zobowiązaniami, a także podejmując działania edukacyjno–informacyjne, skierowane bezpośrednio do użytkowników aplikacji mobilnych. Za wypełnienie tej deklaracji można uznać konkurs na aplikację mobilną przyjazną prywatności, zorganizowany przez Generalnego Inspektora Ochrony Danych Osobowych wspólnie z Ministerstwem Administracji i Cyfryzacji, o czym była już mowa w innej części niniejszego *Sprawozdania*.

Podkreślenia wymaga współpraca Generalnego Inspektora Ochrony Danych Osobowych z Interdyscyplinarnym Centrum Modelowania Matematycznego i Komputerowego (ICM) działającym na Uniwersytecie Warszawskim, nad projektem pod nazwą **System Analizy Orzeczeń Sądowych (SAOS)**. Celem tego systemu jest integracja danych na temat orzeczeń sądów powszechnych, sądów administracyjnych, Sądu Najwyższego i Trybunału Konstytucyjnego oraz stworzenie takich narzędzi analityki publicznej, które umożliwią ponowne wykorzystanie informacji zawartych w orzeczeniach tych sądów (re-use). Dostępność tych informacji jest kluczowa dla całego społeczeństwa, zarówno od strony działalności prawodawczej, analizy działania państwa, jak i stosowania prawa. W ramach projektu wypracowane zostaną rekomendacje dotyczące standardu struktury dokumentu elektronicznego dla wymiaru sprawiedliwości, z możliwością połączenia takich dokumentów z dokumentami elektronicznymi wykorzystywanymi w procesie stanowienia prawa. W ramach szeroko pojętego wymiaru sprawiedliwości funkcjonują różne, niezależne zasady anonimizacji orzeczeń, które utrudniają ustrukturyzowanie treści orzeczeń

w sposób umożliwiający łatwiejsze wydobycie z nich istotnych informacji o prawie. Dlatego wspomniany projekt wychodzi naprzeciw odczuwanemu w Polsce brakowi jednolitych standardów anonimizacji dokumentów elektronicznych administracji publicznej. Generalny Inspektor Ochrony Danych Osobowych niejednokrotnie wskazywał bowiem na konieczność opracowania jednolitych zasad anonimizacji nie tylko w kontekście publikacji wyroków sądowych, ale każdego innego rodzaju informacji publicznej. Definicja taka stanowiłaby gwarancję poszanowania prawa do prywatności i ochrony danych osobowych.

O tym, jak ważne dla różnych podmiotów jest stanowisko organu ds. ochrony danych w sprawach związanych z rozwojem nowoczesnych technologii, świadczy współpraca Generalnego Inspektora Ochrony Danych Osobowych z Komisją Innowacyjności i Nowoczesnych Technologii Sejmu RP. Plan pracy Komisji opracowywany jest w porozumieniu z Generalnym Inspektorem w zakresie zagadnień problemowych, które następnie omawiane są na posiedzeniach tego organu. Dotychczas przedmiotem prac Komisji Innowacyjności i Nowoczesnych Technologii były zagadnienia bezpieczeństwa danych przetwarzanych w chmurach (*cloud computing*), wyzwania Internetu przedmiotów (*Internet - of things*) oraz zagrożenia prywatności związane z wdrażaniem technologii RFID. Przedmiotowe spotkania odbywały się z udziałem Generalnego Inspektora Ochrony Danych Osobowych i jego przedstawiciela. Podczas posiedzenia, podczas którego debatowano nad bezpieczeństwem danych przetwarzanych w chmurach, Generalny Inspektor Ochrony Danych Osobowych zaznaczył, że choć rynek podmiotów dostarczających usługę cloud computing cały czas się kształtuje, to z pewnością w niedługim czasie będzie stanowił większość usług sieciowych i dlatego warto jest zadbać o rozwiązania zapewniające pełne gwarancje poufności i wiarygodności przetwarzania danych. Natomiast w odniesieniu do koncepcji Internetu przedmiotów, wedle której przedmioty jednoznacznie identyfikowalne mogą bezpośrednio lub pośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem sieci komputerowej, wskazał nie tylko na znaczenie gospodarcze tej koncepcji, ale także na jej rolę w budowaniu sieci społecznej. Z kolei o zagrożeniach prywatności związanych z wdrażaniem RFID, Generalny Inspektor Ochrony Danych Osobowych wielokrotnie zabierał głos sygnalizując konieczność projektowania i wykorzystania tej technologii w sposób dopuszczalny z punktu widzenia prawa, etyki oraz zasad społecznych, w szczególności z poszanowaniem prawa do prywatności i zapewnieniem ochrony danych osobowych.

W 2014 r. Generalny Inspektor Ochrony Danych Osobowych pełnił funkcję eksperta w sprawach prowadzonych przez instytucje publiczne. Za przykład może posłużyć udział

GIODO w spotkaniu eksperckim poświęconym kwestii zgodności przepisów prawa polskiego z przepisami Konwencji o ochronie praw człowieka i godności istoty ludzkiej w odniesieniu do biologii i medycyny, które na zaproszenie Pełnomocnika Rządu do Spraw Równego Traktowania odbyło się w Kancelarii Prezesa Rady Ministrów 18 lutego 2014 r. Podczas tego spotkania omawiane były kwestie związane z interpretacją przepisów prawa pod kątem problematyki zgody na interwencje medyczne, pobieraniem narządów dla celów przeszczepienia oraz zakazem osiągania zysku i wykorzystywaniem części ludzkiego ciała w kontekście ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi. Generalny Inspektor Ochrony Danych Osobowych uczulił uczestników spotkania na kwestie związane z wysokim reżimem ochrony danych osobowych w odniesieniu do informacji dotyczących zdrowia. W podobnej roli wystąpił również podczas Konferencji pt. „Gruźlica powraca – prawda czy mit", zorganizowanej w Krakowskim Szpitalu Specjalistycznym im. Jana Pawła II (26.02.2014 r.). Celem Konferencji było przygotowanie wytycznych dla dyrektorów szkół i placówek oświatowych województwa małopolskiego na wypadek pojawienia się w ich otoczeniu osób chorych na gruźlicę oraz przygotowanie odpowiedniej procedury działania w obliczu tego zjawiska. Omówione zostały zagadnienia ochrony danych osobowych pacjenta, jego rodziny i osób postronnych, konsekwencje błędu działania zarówno w zakresie ochrony sanitarno-higienicznej, jak i ustawy o ochronie danych osobowych, udrożnienia systemu wzajemnej komunikacji – szkoła, sanepid, lekarz rodzinny lub inny specjalista działający w danym terenie, z punktu widzenia przepisów o ochronie danych osobowych.

Podkreślenia wymaga również współpraca Generalnego Inspektora Ochrony Danych Osobowych z podmiotami działającymi na polu szeroko rozumianego bezpieczeństwa państwa i obywateli. Zaliczyć do nich należy Polską Platformę Bezpieczeństwa Wewnętrznego (PPBW) i udział GIODO oraz jego przedstawicieli w wydarzeniach organizowanych przez ten podmiot, a także Wyższą Szkołą Policji w Szczytnie (WSP) - gospodarza i organizatora wielu przedsięwzięć, którym GIODO patronuje i uczestniczy w nich jako prelegent. Przykładem może być udział Generalnego Inspektora Ochrony Danych Osobowych w cyklicznie organizowanych przez WSP w Szczytnie konferencjach zarządzania ciągłością działania, których ideą jest koordynacja badań i wymiana informacji na temat zintegrowanych prac badawczych nad technologiami przydatnymi w pracy służb i instytucji odpowiedzialnych za bezpieczeństwo i porządek prawny. Do ww. grona zaliczyć trzeba także Rządowe Centrum Bezpieczeństwa, które w 2014 r. było gospodarzem seminarium dotyczącego wykorzystania biometrii i innych nowoczesnych technologii w ochronie

infrastruktury krytycznej, podczas którego Generalny Inspektor Ochrony Danych Osobowych zapoznał słuchaczy z prawnymi aspektami przetwarzania danych osobowych w systemach biometrycznych.

Co więcej, od wielu lat Generalny Inspektor Ochrony Danych Osobowych współpracuje z Krajowym Stowarzyszeniem Ochrony Informacji Niejawnych, a także Stowarzyszeniem Wspierania Bezpieczeństwa Narodowego, udzielając merytorycznego wsparcia różnym inicjatywom z zakresu doskonalenia ochrony informacji niejawnych i danych osobowych oraz innych tajemnic prawnie chronionych, w szczególności poprzez udział w cyklu konferencji poświęconych bezpieczeństwu narodowemu. W 2014 r. brał udział w debacie ekspertów na temat „Bezpieczeństwo Narodowe – aktualne wyzwania i zagrożenia" podczas V Konferencji Bezpieczeństwa Narodowego, poświęconej zarówno rozwiązaniom technologicznym w zapewnieniu niezakłóconego funkcjonowania obiektów infrastruktury krytycznej, jak i szeroko rozumianej kulturze bezpieczeństwa, przekładającej się na bezpieczeństwo państwa oraz bezpieczeństwo wewnętrzne kraju i całej UE. Uczestniczył ponadto w jubileuszowej Konferencji zorganizowanej z okazji 15-lecia uchwalenia przez Sejm RP ustawy o ochronie informacji niejawnych, pt. „Przeszłość, teraźniejszość i przyszłość ochrony informacji niejawnych w zapewnieniu bezpieczeństwa narodowego RP", poświęconej omówieniu jej znaczenia dla obronności i bezpieczeństwa Państwa. Wśród uczestników tego spotkania znaleźli się interesariusze odpowiedzialni za bezpieczeństwo podmiotów składających się na strukturę krytyczną Państwa Polskiego.

W kręgu szczególnej uwagi Generalnego Inspektora Ochrony Danych Osobowych znajdują się też zagadnienia bezpieczeństwa cyberprzestrzeni, zwłaszcza te, koncentrujące się na szukaniu rozwiązań chroniących administrację publiczną i przedsiębiorstwa przed cyberprzestępczością. Punktem wyjścia jest tu Strategia Komisji Europejskiej w zakresie przeciwdziałania cyberprzestępczości i ochronie danych osobowych oraz wnioski wypływające z ogłoszonej 5 listopada 2014 r. przez Prezydenta RP, **Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej**[478].

W tym miejscu warto również wspomnieć, że Generalny Inspektor Ochrony Danych Osobowych wszedł w skład **Zespołu Zadaniowego ds. ochrony cyberprzestrzeni RP**, który decyzją Ministra Administracji i Cyfryzacji powołany został w dniu 13 czerwca 2014 r. Zespół odpowiedzialny jest za koordynację działań w obszarze bezpieczeństwa

[478] http://www.prezydent.pl/aktualnosci/wydarzenia/art,3063,strategia-istotna-wobec-zmian-na-wschodzie.html

cyberprzestrzeni RP oraz za przygotowanie rekomendacji z tym związanych. Najważniejszym tematem pierwszego inauguracyjnego spotkania Zespołu (28-29.07.2014 r.) były kwestie organizacyjne związane z opracowaniem harmonogramu działań w zakresie zapewnienia bezpieczeństwa, przewidzianego w „Polityce ochrony cyberprzestrzeni RP". Kolejne spotkania poświęcone będą zarówno kwestiom systemowym, jak też analizie danych dotyczących aktualnego stanu zabezpieczenia przed ewentualnymi cyberatakami oraz zidentyfikowanych zagrożeń. Przedstawiciele poszczególnych instytucji wchodzących w skład Zespołu, mają przedstawić ww. informacje na potrzeby przygotowywanego planu działań.

Podkreślenia wymaga również udział Generalnego Inspektora Ochrony Danych osobowych w cyklu konferencji naukowych odbywających się w ramach projektu badawczo-rozwojowego na rzecz bezpieczeństwa i obronności państwa pod nazwą „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", realizowanego przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Uniwersytet Wrocławski, Narodowe Centrum Badań i Rozwoju, Naukowe Centrum Prawno Informatyczne oraz Wydawnictwo C.H. Beck. Wspomniane konferencje przebiegały pod hasłem „Jawność i tajność a sprawność administrowania" (Warszawa, 23.05.2014), „Perspektywy zmian regulacji jawności i jej ograniczeń" (Sejm RP, 20.10.2014), czy „Jawność i ograniczenia jawności publicznych zasobów informacyjnych" (Kazimierz Dolny, 20-22.10.2014).

Celem konferencji było zidentyfikowanie obszarów, w których najczęściej dochodzi do konfliktu jawności i skuteczności, analiza istoty tego zagadnienia oraz przedstawienie propozycji rozwiązań. Podczas tych spotkań prezentowane były m.in. opinie o projektowanej europejskiej regulacji Wzorcowych Przepisów Postępowania Administracyjnego UE w kontekście aktualnych problemów polskiej legislacji związanych z informacją w postępowaniu administracyjnym i sądowym, w tym postulaty zmian polskiego prawa. W szczególności miałyby one dotyczyć przeciwdziałania nadużyciom prawa do informacji, cyberprzestępczości, zasad finansowania i ponownego wykorzystania publicznych baz danych, a także problematyce interoperacyjności rejestrów publicznych w kontekście ochrony bezpieczeństwa i porządku publicznego, w tym zasad przepływu informacji pomiędzy organami publicznymi. Omawiano ponadto kwestie zapewnienia czytelnych kryteriów ustawowych w obszarze rodzajów środków kontroli operacyjnej i ich stosowania oraz niedookreśloności regulacji prawnej, co do sposobu wskazywania katalogu przestępstw wchodzących w zakres stosowania takich środków, a także zagadnienia związane z

problemem niezależnej kontroli retencji danych w warunkach krajowej regulacji prawnej oraz ochrony informacji poufnych i innych materiałów znajdujących się w dyspozycji służb ochrony państwa.

W kręgu zainteresowania uwagi GIODO wciąż pozostaje temat **monitoringu**, a w szczególności brak ustawy o monitoringu, który utrzymuje stan niepewności prawnej niekorzystny zarówno dla tych, którzy rejestrują obraz, jak i dla osób nagrywanych. Obowiązujący w Polsce zakres prawnych podstaw monitoringu wizyjnego odnosi się jedynie do wybranych aspektów jego zastosowania. Podstawy prawne rejestracji obrazu (w niektórych przypadkach również dźwięku) posiadają służby odpowiedzialne za bezpieczeństwo państwa lub porządek publiczny. Wciąż brak jest natomiast uregulowań w tym zakresie w odniesieniu do innych podmiotów państwowych, a także podmiotów prywatnych, w tym osób fizycznych. Wyjątek stanowią regulacje obejmujące określone sfery życia społecznego lub stanowiące podstawę do rejestracji w określonych miejscach. Ponadto kwestia dotycząca rejestracji obrazu i dźwięku w odniesieniu do czynności procesowych uregulowana została w art. 147 Kodeksu postępowania karnego. W opinii Generalnego Inspektora brak kompleksowego uregulowania kwestii dotyczących zasad instalowania i korzystania z systemów monitoringu wizyjnego przez instytucje państwowe, samorządowe i szeroko rozumiane podmioty prywatne, przy jednoczesnej powszechności występowania i zwiększającymi się możliwościami technicznymi w tym zakresie, stanowi zagrożenie dla zagwarantowanych w Konstytucji RP praw i wolności obywatelskich[479], w tym prawa do prywatności i ochrony danych osobowych oraz prawa dostępu do informacji. Generalny Inspektor Ochrony Danych Osobowych zwraca uwagę na konieczność ustawowego unormowania zasad, które stałyby na straży konstytucyjnych praw obywatelskich, poprzez określenie m.in. zakresu podmiotów uprawnionych do stosowania monitoringu w przestrzeni publicznej, praw osób, których wizerunki zostały zarejestrowane, form oznaczania przestrzeni monitorowanej, jako sposobu informowania obywateli o tym obszarze, wymogów wobec administratorów systemów monitoringu w zakresie bezpieczeństwa systemów oraz zarejestrowanych danych, terminów i sposobów retencji danych, ich przetwarzania, udostępniania i niszczenia, a także zakazu stosowania monitoringu w miejscach, w których

[479] Art. 7 – zasada państwa prawnego, Art. 30 – zasada poszanowania i ochrony godności człowieka, Art. 47 – prawo do ochrony prawnej życia prywatnego, Art. 51 – zasada autonomii informacyjnej. Wszelkie ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw (Art. 31 ust. 3).

mogłoby to naruszać godność ludzką. Realizacja tych zasad przyczyni się zarówno do realizacji ochrony wartości konstytucyjnych w zakresie podstawowych praw obywatelskich, w tym ochrony danych osobowych i prywatności, przy jednoczesnym zapewnieniu skutecznych zasad monitoringu wizyjnego na rzecz zapewnienia bezpieczeństwa i porządku publicznego. Podsumowując, w opinii GIODO ważne jest, aby monitoring zbyt głęboko nie ingerował w sferę prywatności człowieka oraz by był stosowany tylko wtedy, gdy w inny sposób nie można zapewnić bezpieczeństwa.

W tym miejscu wskazać należy na zaangażowanie GIODO w prace na rzecz rozwoju **inteligentnych miast i społeczności.** W 2014 r. Generalny Inspektor Ochrony Danych Osobowych został członkiem Forum Strategicznego Centrum Zaawansowanych Technologii Miasta Przyszłości – CZTMP, działającego przy Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie. Podstawowym zadaniem CZTMP jest integracja i koordynacja aktywności i działań służących wypracowywaniu i rozpowszechnianiu innowacyjnych rozwiązań opartych m.in. na zintegrowanych technologiach informacyjno-komunikacyjnych.

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

Rok 2014 przyniósł nowelizację ustawy o ochronie danych osobowych. Wchodzące w życie nowe przepisy m.in. doprecyzowały wymagania w stosunku do administratorów bezpieczeństwa informacji (ABI), jak i ich role i zadania. Decyzja o powołaniu ABI będzie należała do administratora danych, który jeśli uzna, że jest w stanie samodzielnie zadbać o prawidłowe przetwarzanie danych osobowych i sprawować pełną kontrolę nad tym procesem, nie musi tego robić.

Niemniej jednak w opinii Generalnego Inspektora Ochrony Danych Osobowych warto rozważyć przyjęcie tego nowego rozwiązania proponowanego przez ustawodawcę i skorzystać z profesjonalnej pomocy ABI. Należy bowiem podkreślić, że chodzi tutaj o osoby, które odpowiadają nie tylko za kwestie techniczne związane np. z szyfrowaniem danych czy prawidłowym zabezpieczeniem systemów informatycznych przed atakami cyberprzestępców. ABI ma bowiem odpowiadać za całokształt prawidłowego przetwarzania danych, a więc zarówno za ich ochronę i bezpieczeństwo, jak i szkolenia oraz doradzanie pracownikom administratora mającym do nich dostęp. ABI ma nadzorować cały proces przetwarzania

danych w instytucji. Dlatego zdaniem Generalnego Inspektora warto byłoby skorzystać z tej instytucji i potraktować okres między obowiązywaniem znowelizowanych przepisów ustawy o ochronie danych osobowych a wejściem w życie unijnego rozporządzenia, jako czas na naukę i przygotowanie się do tym zmian.

Rok 2014 kolejnym rokiem wytężonych prac legislacyjnych nad reformą prawa ochrony danych osobowych w Unii Europejskiej. Unia Europejska znajduje się w punkcie zwrotnym wprowadzenia nowych ram ochrony danych dostosowanych do potrzeb XXI wieku, przewidujących wysoki poziom ochrony danych osobowych. Reforma systemu ochrony danych osobowych pozostawała na przestrzeni ostatnich lat wysoko na liście priorytetów działalności GIODO. Konieczność uporządkowania dyskusji nad projektami i zapewnienie właściwego przedstawienia sprawy opinii publicznej było powodem podjęcia przez Generalnego Inspektora szeregu działań na szczeblu krajowym (konferencje, seminaria, konsultacje), aby informacje na ten temat przeniknęły do świadomości społecznej.

Generalny Inspektor Ochrony Danych Osobowych prowadził więc na ten temat konsultacje z przedstawicielami sektora prywatnego i publicznego. Byli to między innymi przedstawiciele policji i sądownictwa, regulatorzy łączności elektronicznej, organizacje społeczeństwa obywatelskiego oraz środowiska akademickie. GIODO odbył szereg spotkań i konsultacji z różnymi podmiotami krajowymi, zainteresowanymi tym zagadnieniem. Wśród nich znaleźli się przedstawiciele sektora telekomunikacji i IT zrzeszonych w Polskiej Izbie Informatyki i Telekomunikacji, środowiska bankowego (Związku Banków Polskich, Biura Informacji Kredytowej), prawniczego – w tym Krajowej Rady Sądowniczej, Polskiej Izby Ubezpieczeń oraz Polskiej Organizacji Handlu i Dystrybucji. Waga sygnalizowanych przez te podmioty kwestii okazała się bardzo znacząca w kontekście dalszych prac nad unijnym projektem oraz planowanych zmian w polskich przepisach prawa o ochronie danych osobowych. Założenia reformy ochrony danych osobowych były również przedmiotem dyskusji prowadzonej na Konferencji pt. Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne, zorganizowanej w styczniu 2015 r. przez Generalnego Inspektora Ochrony Danych Osobowych w związku z obchodami IX Dnia Ochrony Danych Osobowych.

Unijna reforma ochrony danych ma na celu stworzenie nowoczesnych, solidnych, spójnych i kompleksowych ram ochrony danych w Unii Europejskiej. Przyniesie ona korzyści przede wszystkim osobom fizycznym poprzez wzmocnienie ich praw do ochrony danych osobowych oraz zaufania do środowiska cyfrowego. W znacznym stopniu uprości też

środowisko prawne dla przedsiębiorstw i sektora publicznego, co niewątpliwie pobudzi rozwój gospodarki cyfrowej na całym jednolitym rynku UE i poza nim, zgodnie z celami unijnej strategii „Europa 2020" i Europejskiej Agendy Cyfrowej. Ponadto reforma zwiększy wzajemne zaufanie organów ścigania, co ułatwi wymianę danych między nimi oraz współpracę w zakresie zwalczania poważnej przestępczości, zapewniając przy tym wysoki poziom ochrony osobom fizycznym.

Z perspektywy organu ochrony danych szczególnie istotne jest aby projektowane rozporządzenie nie obniżało poziomu ochrony danych zapewnianego przez obecnie obowiązującą dyrektywę 95/46WE. Dorobek wspólnotowy oparty na prawach podstawowych powinien pozostać nietknięty. Oczywiście przepisy powinny zapewniać elastyczność, tak jak na przykład przyznanie państwom członkowskim uprawnienia w takich kwestiach jak ochrona zdrowia, badania statystyczne etc. Przepisy musza też nadążać za rozwojem cywilizacyjnym i być dostosowane do postępu technologicznego. Jednak – zdaniem organu ochrony danych – nie powinno to prowadzić do obniżenia poziomu ochrony.

Przyszły system ochrony danych osobowych powinien zapewniać jasne i zrozumiałe przepisy prawne. Zbyt często prawa dotyczące prywatności sprawiały wrażenie skomplikowanych, zbyt wyszukanych oraz zrozumiałych tylko przez wąskie kręgi ekspertów. Mając na uwadze potrzebę zapewnienia wszystkim osobom, których dane dotyczą możliwość kontroli nad ich danymi, z jednej strony zaś uproszczenie biurokratycznych obciążeń dla przedsiębiorców, z drugiej strony – głównym zadaniem nowego rozporządzenia jest uproszczenie przepisów.

Rozporządzenie nie powinno ograniczać innowacji, a wręcz przeciwnie powinno ją wspierać. Ochrona danych może pomóc zbudować zaufanie w społeczeństwie cyfrowym, w efekcie oferując prawdziwą, konkurencyjną przewagę. Dlatego też zasada rozliczalności za przetwarzanie danych powinna być promowana jako nowe podejście do usuwania barier biurokratycznych.

Nowe przepisy wzmocnią rolę organów ochrony danych, ujednolicając ich uprawnienia i kompetencje, aby jeszcze skuteczniej zagwarantować, a w razie konieczności zapewnić przestrzeganie zgodności z prawem, zarówno indywidualnie na poziomie krajowym, jak i we współpracy ze sobą, na przykład, poprzez nakładanie znacznych kar finansowych. Środki te umożliwią skuteczną realizację egzekwowania prawa przez organy ochrony danych.

Jednocześnie pojawiło się wiele nowych tematów, które wywarły duży wpływ na przyszłość ochrony danych osobowych. Jednym z nich była informacja o masowej inwigilacji

Europejczyków w ramach programu PRISM, czy wzrastająca liczba zastrzeżeń co do przejrzystości i realnych gwarancji właściwego przetwarzania danych osobowych obywateli państw europejskich przez firmy amerykańskie w ramach programu „Safe Harbour". Stąd rok 2014 był czasem przeglądu zasad programu, co wcześniej zapowiedziała Komisja Europejska w swoim komunikacie.

Generalny Inspektor Ochrony Danych Osobowych ma świadomość tego, że dla urzeczywistnienia prawa jednostki do poszanowania jej prawa do prywatności i ochrony danych osobowych nie wystarczy sama ochrona prawna. Obowiązek zachowania szczególnej ostrożności i staranności w procesie przetwarzania danych osobowych, spoczywa w równym stopniu na administratorze danych, jak i na osobie, których dane te dotyczą. Ani przepisy prawa, ani Generalny Inspektor Ochrony Danych Osobowych nie uchronią obywatela przed przejęciem jego danych przez nieuprawniony podmiot, o ile on sam nie zadba o ochronę swoich danych i nie będzie z nimi właściwie postępować, stosując się do zasad bezpieczeństwa.

Dowodzą tego wyniki badań **przeprowadzonych na potrzeby kampanii „Nie daj się okraść. Chroń swoją prywatność"**, które przedstawione zostały podczas konferencji prasowej GIODO w ramach trwającego **Tygodnia Zapobiegania Kradzieży Tożsamości.** Pokazały one, że choć problem kradzieży tożsamości istnieje w świadomości badanych jednostek, to jednak w małym stopniu wpływa na ich postawy i zachowania związane z ochroną danych. Potwierdziło to porównanie badań przeprowadzonych we wcześniejszych latach (2005, 2006, 2007, 2010) w Warszawie oraz we Wrocławiu, dotyczących postępowania zarówno z dokumentacją papierową, jak i zabezpieczania dokumentów tożsamości oraz nośników informatycznych zawierających dane osobowe. Jednostkowe odpowiedzi badanych osób na temat zabezpieczania dokumentów były bardzo pozytywne, co jednak nie przekładało się na odpowiedzialne postępowanie tych osób w konkretnych sytuacjach. Mimo iż badani deklarowali dbałość o zabezpieczenie zbędnej dokumentacji zawierającej dane osobowe, to aż połowa z nich oświadczyła, że wyrzuca taką dokumentację bezpośrednio do śmietnika ograniczając się jedynie do jej przedarcia, zaś 9 % badanych w całości wyrzuca dokumenty do kosza. Podobnie respondenci zachowywali się podczas korzystania z Internetu. Jedynie 37 % badanych było w nim całkowicie anonimowa, zaś ponad połowa (51 %) udostępniła swoje dane osobowe innemu Internaucie, narażając się tym samym na niebezpieczeństwo kradzieży tożsamości. Z kolei z badania przeprowadzonego na terenie Miejskiego Przedsiębiorstwa Oczyszczania (MPO) w Warszawie, podczas którego przeanalizowano zawartość 4-tonowego

kontenera z makulaturą wynikało, że wśród pochodzących z biur dokumentów niezniszczonych było aż 93 %, zaś tych z domów prywatnych pochodziło 87 %.

Analiza zachowań respondentów w połączeniu z wynikami badań pozwoliła wysnuć wniosek, że zarówno osoby prywatne, jak i firmy nie przywiązują należytej uwagi do zabezpieczenia dokumentacji i urządzeń zawierających dane osobowe[480]. Świadomość zagrożeń związanych z kradzieżą tożsamości to tylko połowa sukcesu, za którym powinny pojawić się konkretne przykłady dobrych praktyk. Stąd przed organem ochrony danych osobowych stoi wciąż aktualne zadanie edukacji społeczeństwa i potrzeba zintensyfikowania działań GIODO w tym właśnie kierunku.

Podobnej reakcji organu ds. ochrony danych osobowych wymaga kwestia podniesienia świadomości z zakresu prawa do prywatności i ochrony danych osobowych wśród przedstawicieli zawodów prawniczych. Zagadnienia ochrony danych osobowych sędziów, zakres informacji udostępnianych o sędziach w ramach dostępu do informacji publicznej oraz granice ingerencji w prywatność osób pełniących funkcje publiczne wciąż są przedmiotem niejasności interpretacyjnych wymagających rozstrzygnięć NSA. Do tego wymienić należy także kwestie związane z informatyzacją sądownictwa, które mają znaczący wpływ na realizację prawa do ochrony danych osobowych w działalności orzeczniczej i w codziennym funkcjonowaniu sądów. Podkreślenia bowiem wymaga, że sąd jest administratorem danych osobowych zarówno osób w nim zatrudnionych, jak i tych, których dane pozyskuje w związku z prowadzonymi postępowaniami.

Wspomnieć także należy, że kwestia samego procesu informatyzacji sądownictwa stała się dla organu ds. ochrony danych osobowych przedmiotem szczególnej uwagi już z chwilą opiniowania w 2012 r. ***projektu rozporządzenia Ministra Sprawiedliwości zmieniającego rozporządzenie – Regulamin urzędowania sądów powszechnych***. Wypowiadając się krytycznie względem objęcia tak istotnej sprawy, jaką jest informatyzacja sądownictwa, materią rozporządzenia, przyczynił się do rozpoczęcia właściwych prac legislacyjnych poświęconych temu tematowi, tj. prac nad ***projektem ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych***[481].

---

[480] Badania przeprowadzone były w okresie od 22.10.2013 r. do 4.10.2014 r. W ciągu roku ankietę wypełniło 1107 badanych. Więcej na temat badań zob. http://giodo.gov.pl/1520195/id_art/8189/j/pl .

[481] Uwagi GIODO zgłoszone względem *projektu ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych* można znaleźć na stronie internetowej Rządowego Centrum Legislacji pod adresem: www.rcl.gov.pl .

I tak, w ocenie Generalnego Inspektora Ochrony Danych Osobowych kwestia wokand (w tym także e-wokand) wymaga niezwłocznych działań legislacyjnych mających na celu rzetelne i szczegółowe unormowanie kwestii ujawniania danych osobowych na wokandach sądowych w zależności od jawności rozprawy lub rodzaju sprawy. Bowiem **prawo do zamieszczania danych osobowych na wokandach sądowych nie może wynikać z przepisów o charakterze wewnętrznym** – w tym przypadku z treści zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej (Dz. Urz. MS Nr 5, poz. 22 z późn. zm.)[482]. Przepisy przywołanego zarządzenia, regulując treść wokandy sądowej, determinują w istocie kwestię przetwarzania danych osobowych stron postępowania, naruszając w ten sposób prawo człowieka do nieujawniania informacji dotyczących jego osoby bez zobowiązania ustawowego. Co więcej, w aktualnie obowiązującym stanie prawnym brak jest też podstaw do zamieszczania treści wokand sądowych w Internecie. Stąd wskazywana przez GIODO konieczność rzetelnego i precyzyjnego uregulowania w akcie prawnym o randze ustawy, kwestii dotyczącej zarówno treści wokandy, jak i sposobu jej udostępniania.

W 2014 r. Generalny Inspektor Ochrony Danych Osobowych oraz jego przedstawiciele uczestniczyli w spotkaniach, konferencjach i debatach poświęconym tym zagadnieniom, organizowanym zarówno przez ośrodki uniwersyteckie, jak i stowarzyszenia prawnicze czy sądy. Co więcej, Generalny Inspektor już w 2013 roku wspólnie z Krajową Radą Radców Prawnych zainicjował cykl szkoleń z zakresu ochrony i bezpieczeństwa danych w kancelariach prawnych. W 2014 roku GIODO przeprowadził 19 takich szkoleń w Okręgowych Izbach Radców Prawnych w kilkunastu miastach Polski. Ponadto wśród podmiotów szkolonych znaleźli się także doradcy podatkowi z szesnastu regionalnych oddziałów Krajowej Izby Doradców Podatkowych, prokuratorzy i urzędnicy Prokuratury Okręgowej w Warszawie, Sądu Okręgowego w Gdańsku oraz aplikanci aplikacji legislacyjnej.

Szerokie wykorzystanie technologii informacyjno-komunikacyjnych praktyczne we wszystkich dziedzinach życia i działalności społecznej, a zwłaszcza powszechne włączanie technologii cyfrowych w obszary codziennej aktywności człowieka, spowodowało, że

[482] Zgodnie z Art. 93 ust. 1 Konstytucji RP uchwały Rady Ministrów oraz rozporządzenia Prezesa Rady Ministrów i ministrów mają charakter wewnętrzny i obowiązują tylko jednostki organizacyjne podległe organowi wydającemu te akty. W myśl Art. 93 ust. 2 Konstytucji, zarządzenia są wydawane tylko na podstawie ustawy. Nie mogą one stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów.

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. Dlatego tak bardzo ważne jest, aby wykorzystywanie informacji na ich temat przez inne podmioty odbywało się w sposób przejrzysty, odpowiedzialny i kontrolowany. Wzrasta bowiem świadomość obywateli w kwestii wykorzystania potencjału nowych technologii na poprawę jakości ich życia we wszystkich wymienionych obszarach, zaś transakcje przeprowadzane na pozbawionym granic jednolitym rynku cyfrowym pozwalają im docenić prawdziwą wartość Internetu. Ale powinno to iść w parze ze wzrostem świadomości obywateli i wzmocnieniem ich praw w zakresie ochrony prywatności i danych osobowych. Dlatego przed organem ds. ochrony danych osobowych stoi wciąż bardzo ważne i aktualne zadanie - zachęcenia administratorów danych do inwestowania od początku w prawidłową ochronę danych, np. poprzez realizację koncepcji ochrony prywatności w fazie projektowania (*privacy by design*)[483], 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. Należałoby także rozważyć potrzebę opracowania wytycznych w zakresie wzorów umów stosowanych przez podmioty publiczne w zakresie informatyzacji publicznych zbiorów danych osobowych, z zapewnieniem *privacy by design* oraz rzetelnym zabezpieczeniem interesu podmiotu publicznego.

Generalny Inspektor Ochrony Danych Osobowych dostrzega również szereg innych zagadnień związanych z rozwojem nowoczesnych technologii, które wciąż wymagają omówienia i uregulowania. Wśród nich wymienić należy potrzebę wzmocnienia praw osób, których dane ujęte w zbiorach będą udostępniane/pozyskiwane przez organy bezpieczeństwa państwa (a w przyszłości także przez inne podmioty) wyłącznie za pomocą systemów teleinformatycznych (on-line), sygnalizowana wcześniej konieczność wprowadzenia regulacji prawnej dotyczącej usług monitoringu wizyjnego, zagadnienie identyfikacji i uwierzytelnienia w systemach teleinformatycznych administracji publicznej (ze szczególnym uwzględnieniem prac nad rozporządzeniem eIDAS), dostęp do danych geolokalizacyjnych, aplikacje mobilne, ochrona praw jednostek w związku z regulacją stosowania bezzałogowych statków latających

[483] 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.

(tzw. dronów), czy identyfikacja i analiza zagrożeń płynących z upowszechniania rozwiązań opartych na biometrii w kontaktach obywateli z instytucjami publicznymi i prywatnymi.

Wskazuje ponadto na potrzebę rewizji polskiej regulacji dotyczącej retencji danych telekomunikacyjnych w obliczu wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z 8 kwietnia 2014 r. (sygn. akt C-293/12, C-594/12) uznającego tzw. dyrektywę retencyjną za nieważną, wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11) uznającego część przepisów o uprawnieniach służb państwowych za sprzeczne z Konstytucją, a także koncepcję „prawa do bycia zapomnianym" w świetle wyroku TSUE w sprawie Google Spain (C-131/12).

Podkreślenia wymaga również zagadnienie ochrony prywatności w związku z rozwojem Internetu Przedmiotów, który był przedmiotem szczególnej uwagi podczas obrad **36. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności**. W przyjętej wówczas **Deklaracji w sprawie Internetu Przedmiotów**, rzecznicy zwracają uwagę na coraz powszechniej występujące urządzenia podłączone do Internetu, które są w stanie komunikować się między sobą, czego użytkownicy nie zawsze są świadomi. Wprawdzie urządzenia te mogą ułatwić nasze życie prywatne i zawodowe oraz zapewnić rozrywkę, ale równocześnie mogą ujawniać poufne informacje. Dane uzyskane z czujników Internetu Przedmiotów charakteryzują się wysoką jakością i wrażliwością, umożliwiając z wysokim prawdopodobieństwem identyfikację konkretnej osoby. Dlatego przyjęto, że pozyskane tą drogą informacje należy uznać za dane osobowe i objąć je odpowiednią ochroną. I chociaż wielu przedsiębiorstwom ten model biznesowy (tj. Internet Przedmiotów) jest jeszcze nieznany, to jednak wkrótce może się to zmienić. W obecnych czasach połączenie z siecią czy urządzeniami jest rzeczą tak powszechną, że coraz trudniej jest wyobrazić sobie współczesny świat bez takich możliwości komunikacji. W celu zagwarantowania skutecznej ochrony prywatności i danych osobowych użytkowników Internetu Przedmiotów, konieczna jest wspólna odpowiedzialność wszystkich interesariuszy - w społeczeństwie, aby utrzymać zaufanie do tych połączonych systemów. W tym celu kluczowa jest przejrzystość. Oferujący urządzenia Internetu Przedmiotów powinni wiedzieć, jakie dane gromadzą, w jakich celach oraz jak długo dane te są zatrzymywane. Powinni wyeliminować sytuacje, w których klienci są zaskakiwani pozakontekstowymi ofertami, na które wyrażają zgodę najczęściej pod wpływem chwili i towarzyszących jej emocjom. Przy zakupie urządzenia lub aplikacji Internetu Przedmiotu, klientowi należy zapewnić odpowiednie, wystarczające i zrozumiałe informacje. Obecne polityki prywatności nie zawsze

zapewniają informacje w zrozumiały sposób. Zgodę udzieloną na podstawie takich polityk trudno jest więc uznać za świadomie wyrażoną. Przedsiębiorstwa muszą zmienić sposób myślenia, aby zapewnić, że polityki prywatności nie będą im służyły wyłącznie do ochrony przed sporami.

Rzecznicy ochrony danych i prywatności zachęcają więc do rozwoju technologii, które będą wprowadzały nowe sposoby ochrony danych osobowych i prywatności konsumenta od samego początku, tj. od momentu zebrania danych. Ochrona prywatności w fazie projektowania (*Privacy by design*) oraz domyślna ochrona prywatności (*Privacy by default*), nie powinny już być traktowane jako coś osobliwego, tylko stać się kluczową cechą innowacyjnych technologii.

Dlatego tak wielka jest rola rzeczników w kwestii właściwego określenia barier w egzekwowaniu prawa do prywatności oraz właściwa identyfikacja ograniczeń prawnych i pozaprawnych, na które napotykają organy ochrony danych w związku z wdrażaniem prawa do prywatności i ochrony danych osobowych, zarówno z punktu widzenia regulatorów, jak i interesariuszy. Ważne jest bowiem przywrócenie zaufania obywateli, wskutek zapewnienia realnych możliwości egzekwowania od wszystkich podmiotów, by przestrzegali zasad.

ZAŁĄCZNIKI:

Załącznik nr 1

Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2014 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.	Rada Miasta Żyrardowa	15.01.2014 DIS-K-421/157/13	Podjęcie działań mających na celu zmianę wzorów deklaracji o wysokości opłaty za gospodarowanie opłatami komunalnymi w zakresie zapewnienia zgodności ww. wzorów deklaracji z przepisami o ochronie danych osobowych.
2.	Rada Miasta Lublin	17.01.2014 DIS-K-421/79/13	Podjęcie działań mających na celu zmianę wzorów deklaracji o wysokości opłaty za gospodarowanie opłatami komunalnymi w zakresie zapewnienia zgodności ww. wzorów deklaracji z przepisami o ochronie danych osobowych.
3.	Rada Gminy Parzęczew	21.01.2014 DRZDO/405/30/14/48075	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
4.	Urząd Miejski w Świeciu	29.01.2014 DOLiS-035-3294/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Stanu Cywilnego w Świeciu w związku z pozyskiwaniem za pomocą wniosku o wydanie zaświadczenia o zdolności prawnej do zwarcie związku małżeńskiego za granicą, dane osobowe w zbyt szerokim, nieadekwatnym do celu zakresie.
5.	Urząd Dzielnicy Ochota m.st. Warszawy	05.02.2014 DOLiS-035-86/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Burmistrza Dzielnicy Ochota Miasta Stołecznego Warszawy w związku z opublikowaniem na stronie internetowej urzędu danych osobowych nabywców lokali mieszkalnych przeznaczonych na sprzedaż.
6.	Poznańskie Ośrodki Sportu i Rekreacji	19.02.2014 DOLiS-035-3623/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Poznańskich Ośrodków Sportu i Rekreacji w związku z zatrzymywaniem dowodów osobistych osób korzystających z lodowiska.
7.	Muzeum Powstania Warszawskiego	20.02.2014 DOLiS-035-4480/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych skierowane do Muzeum Powstania Warszawskiego w związku z faktem, iż dowody osobiste osób odwiedzających Muzeum Powstania Warszawskiego są przechowywane, w zamian za wypożyczenie elektronicznego przewodnika.
8.	Starostwo Powiatowe w Trzebnicy	10.03.2014 DOLiS-035-138/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych skierowane do Starostwa Powiatowego w Trzebnicy w sprawie udostępnienia na stronie internetowej Starostwa numerów ksiąg wieczystych poszczególnych nieruchomości.

9.	Prezes Regionalnej Izby Obrachunkowej	03.04.2014 DIS-K-421/157/13	Podjęcie działań mających na celu zapewnienie zgodności z przepisami o ochronie danych osobowych, wzorów deklaracji o wysokości opłaty za gospodarowanie opłatami komunalnymi.
10.	Przewodnicząca Rady Miejskiej w Łodzi	23.05.2014 DIS-K-421/66/14	Podjęcie działań mających na celu zmianę wzorów deklaracji o wysokości opłaty za gospodarowanie opłatami komunalnymi w zakresie zapewnienia zgodności ww. wzorów deklaracji z przepisami o ochronie danych osobowych.
11.	Urząd Miejski w Lidzbarku Warmińskim	30.05.2014 DOLiS-035-937/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Miejskiego w Lidzbarku Warmińskim w związku z zamieszczaniem imion i nazwisk na stronie internetowej urzędu.
12.	Urząd Gminy Ślemień	05.06.2014 DOLiS-035-1027/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych, skierowane do Urzędu Gminy Ślemień w związku z zamieszczaniem imion i nazwisk w BIP.
13.	Urząd Gminy w Obrazowie	18.06.2014 DOLiS-035-1241/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych, skierowane do Urzędu Gminy w Obrazowie w związku z treścią zamieszczonego na stronie internetowej gminy Obrazów wzoru formularza wniosku o udostępnienie informacji publicznej.
14.	Rada Gminy Rogowo	20.06.2014 DRZDO/405/31/14/48071	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
15.	Rada Gminy Orla	18.07.2014 DRZDO/405/37/14/56514	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
16.	Rada Miejska w Łęczycy	18.07.2014 DRZDO/405/38/14/56516	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
17.	Zgromadzenie Związku Gmin Zagłębia Miedziowego	21.07.2014 DRZDO/405/39/14/56628	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
18.	Ministerstwo Sprawiedliwości	05.08.2014 DOLiS-035-278/14	Wystąpienie do Ministerstwa Sprawiedliwości o podjęcie działań legislacyjnych w zakresie unormowania kwestii ujawniania danych osobowych na wokandach sądowych.
19.	Rada Miejska w Dobrym Mieście	26.08.2014 DRZDO/405/46/14/66963	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
20.	Ośrodek Sportu i Rekreacji m.st. Warszawy w Dzielnicy Ochota	12.09.2014 DOLiS-035-2008/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych skierowane do Ośrodka Sportu i Rekreacji m.st. Warszawy w Dzielnicy Ochota, w związku z pozyskaniem przez GIODO informacji, iż dowody osobiste osób korzystających z infrastruktury Ośrodka (OSiR) są zatrzymywane w zastaw za

			kluczyk do szafki w szatni na czas korzystania z obiektu , jak również długoterminowo, gdy użytkownik zgubi kluczyk.
21.	Urząd Gminy Komorniki	24.09.2014 DOLiS-035-1993/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Gminy Komorniki w związku z publikowaniem w Biuletynie Informacji Publicznej Urzędu Gminy Komorniki danych osobowych osób kierujących skargi do Rady Gminy Komorniki.
22.	Urząd Gminy Wiązowna	26.09.2014 DOLiS-035-2259/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Gminy Wiązowna w związku z opublikowaniu na stronie internetowej gminy danych osobowych osób zwracających się z pytaniami do Wójta.
23.	Centrum Onkologii im. prof. Fr. Łukaszczyka w Bydgoszczy	30.09.2014 DOLiS-035-4806/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Centrum Onkologii im. prof. Fr. Łukaszczyka w Bydgoszczy w związku z zamieszczeniem na stronie internetowej niezanonimizowanego protokołu kontroli przeprowadzonej przez inspektorów pracy Okręgowego Inspektoratu Pracy w Bydgoszczy.
24.	Kujawsko-Pomorski Urząd Wojewódzki w Bydgoszczy	30.09.2014 DOLiS-035-4806/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Kujawsko-Pomorskiego Urzędu Wojewódzkiego w Bydgoszczy w związku z zamieszczeniem na stronie internetowej niezanonimizowanego protokołu kontroli przeprowadzonej przez inspektorów pracy Okręgowego Inspektoratu Pracy w Bydgoszczy.
25.	Urząd Miasta Bydgoszczy	30.09.2014 DOLiS-035-4806/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Miasta Bydgoszczy w związku z zamieszczeniem na stronie internetowej niezanonimizowanego protokołu kontroli przeprowadzonej przez inspektorów pracy Okręgowego Inspektoratu Pracy w Bydgoszczy.
26.	Urząd Gminy Rogowo	30.09.2014 DOLiS-035-4806/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Gminy Rogowo w związku z zamieszczeniem na stronie internetowej niezanonimizowanego protokołu kontroli przeprowadzonej przez inspektorów pracy Okręgowego Inspektoratu Pracy w Bydgoszczy.
27.	Urząd Gminy Nieporęt	03.10.2014 DOLiS-035-2379/14	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Gminy Nieporęt w sprawie wysyłania przez Urząd Gminy Nieporęt do mieszkańców gratulacji z okazji ukończenia 6 urodzin.
28.	Urząd Miasta Katowice	10.10.2014 DOLiS-035-2506/14	Wystąpienie na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych do Prezydenta Miasta Katowice w związku z pozyskaniem przez GIODO informacji o zamieszczeniu na stronie internetowej urzędu numerów ksiąg wieczystych poszczególnych nieruchomości.
28.	Ministerstwo Pracy i Polityki Społecznej	27.10.2014 DOLiS-035-1996/13	Wystąpienie z art. 19a ust. 1 i 2 ustawy o ochronie danych osobowych do Ministerstwa Pracy i Polityki Społecznej o stworzenie aktu prawnego określającego zasady i sposób przetwarzania danych osobowych gromadzonych w rejestrach publicznych w obszarze pomoc społeczna, wspieranie rodziny i piecza zastępcza.

30.	Rada Miejska w Kartuzach	5.11.2014 DRZDO/405/56/14/87491	Podjęcie działań mających na celu zmianę wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie zapewnienia zgodności ww. wzoru deklaracji z przepisami o ochronie danych osobowych.
31.	Rzecznik Praw Obywatelskich	05.11.2014 DOLiS-035-1717/14	Wystąpienie do Rzecznika Praw Obywatelskich o rozważenie skierowania do Trybunału Konstytucyjnego wniosku o zbadanie zgodności przepisów dot. działania rodzinnych ośrodków diagnostyczno-konsultacyjnych.
32.	Przewodniczący Komisji Nadzoru Finansowego	18.11.2014 DIS-K-421/51/14	Podjęcie działań mających na celu zmianę uchwały Komisji Nadzoru Finansowego w sprawie wykazu dokumentów dotyczących działalności gospodarczej przedsiębiorcy lub przedsiębiorcy zagranicznego załączanych do wniosku o udzielenie zezwoleń, o których mowa w art. 6a ust. 1 pkt 1 lit. m oraz art. 6d ust. 1 ustawy Prawo bankowe.
33.	Starostwo Powiatowe w Cieszynie	11.12.2014 DOLiS-035-4646/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Starostwa Powiatowego w Cieszynie w związku z zamieszczeniem niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy Okręgowego Inspektoratu Pracy w Katowicach.
34.	Urząd Miasta w Lędzinach	11.12.2014 DOLiS-035-4646/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Urzędu Miasta w Lędzinach w związku z zamieszczeniem niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy Okręgowego Inspektoratu Pracy w Katowicach.
35.	Centrum Kształcenia Praktycznego w Bażanowicach	11.12.2014 DOLiS-035-4646/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Centrum Kształcenia Praktycznego w Bażanowicach, w związku z zamieszczeniem niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy Okręgowego Inspektoratu Pracy w Katowicach.
36.	Zespół Szkolno-Przedszkolny nr 3 w Tychach	11.12.2014 DOLiS-035-4646/13	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych do Zespołu Szkolno-Przedszkolnego nr 3 w Tychach w związku z zamieszczeniem niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy Okręgowego Inspektoratu Pracy w Katowicach.

Załącznik nr 2

Wykaz kontroli przeprowadzonych w 2014 r.

L.p.	Data / Sygnatura kontroli	Nazwa podmiotu i miejsce kontroli	Inicjatywa kontroli	Rozstrzygnięcie
1.	13-15.01.2014 DIS-K-421/1/14	Wydawnictwo Wiedza i Praktyka Sp. z o.o., Warszawa, ul. Łotewska 9A	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
2.	13-17.01.2014 DIS-K-421/2/14	Biuro Ochrony Rządu, Warszawa, ul. Podchorążych 38	z urzędu	przywrócono stan zgodny z prawem
3.	13-17.01.2014 DIS-K-421/3/14	Zarząd Transportu Miejskiego, Warszawa, ul. Żelazna 61	Departament Orzecznictwa Legislacji i Skarg	11.06.2014 decyzja DIS/DEC-551/14/44895
4.	13-15.01.2014 DIS-K-421/4/14	Komisja do Zwalczania Dopingu w Sporcie, Warszawa,- ul. Łazienkowska 6A	z urzędu	17.07.2014 decyzja DIS/DEC-676/14/55359
5.	20-24.01.2014 DIS-K-421/5/14	Edoktor.pl Sp. z o.o., Warszawa,ul. Fieldorfa 10/70	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
6.	20-24.01.2014 DIS-K-421/6/14	Designet Sp. z o.o., Warszawa, ul. Indiry Gandhi 35/6	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
7.	20-24.01.2014 DIS-K-421/7/14	Pure Health and Fitness Sp. z o.o., Warszawa,ul. Złota 59	Departament Orzecznictwa Legislacji i Skarg	06.11.2014 decyzja DIS/DEC-1072/14/87525
8.	21-23.01.2014 DIS-K-421/8/14	D-Force Sp. z o.o., Warszawa, ul. Narbutta 82/84	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
9.	27-31.01.2014 DIS-K-421/9/14	Polskie Linie Lotnicze LOT S.A., Warszawa, ul. 17 Stycznia 39	z urzędu	04.06.2014 decyzja DIS/DEC-521/14/42854
10.	27-30.01.2014 DIS-K-421/10/14	Prezydent m.st. Warszawy, Warszawa, Plac Bankowy 3/5	z urzędu	26.06.2014 decyzja DIS/DEC-600/14/48641
11.	03-06.02.2014 DIS-K-421/11/14	Ministerstwo Finansów, Warszawa,ul. Świętokrzyska 12	z urzędu	01.07.2014 decyzja DIS/DEC-623/14/49897,49899
12.	03-07.02.2014 DIS-K-421/12/14	Polski Związek Podnoszenia Ciężarów, Warszawa,ul. Marymoncka 34	z urzędu	nie stwierdzono uchybień
13.	03-07.02.2014 DIS-K-421/13/14	Urząd Miasta Dzierżoniów, Dzierżoniów, ul. Rynek 1	Departament Orzecznictwa Legislacji i Skarg	09.05.2014 decyzja DIS/DEC-446/14/35683
14.	03-07.02.2014 DIS-K-421/14/14	Wojewódzki Szpital Zespolony w Koninie, Konin, ul. Szpitalna 45	Departament Orzecznictwa Legislacji i Skarg	13.05.2014 decyzja DIS/DEC-454/14/36247
15.	10-13.02.2014 DIS-K-421/15/14	Dawid Olejniczak prowadzący działalność gospodarczą pod nazwą „CreaMedia Dawid Olejniczak", Włocławek, ul. Piekarska 2/2	Departament Orzecznictwa Legislacji i Skarg	23.10.2014 decyzja DIS/DEC-1012/14/82855
16.	10-14.02.2014 DIS-K-421/16/14	87 RS Mobcomer GT Sp. z o.o., Warszawa, Al. Jerozolimskie 56C	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg

17.	10-14.02.2014 DIS-K-421/17/14	87 RS Mobcomer GT Sp. z o.o., Warszawa, Al. Jerozolimskie 56C	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
18.	10-14.02.2014 DIS-K-421/18/14	87 RS Mobcomer GT Sp. z o.o., Warszawa, Al. Jerozolimskie 56C	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
19.	10-12.02.2014 DIS-K-421/19/14	Mediadress Polonia Sp. z o.o., Skierniewice, ul. Unii Europejskiej 20	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
20.	17-20.02.2014 DIS-K-421/20/14	Instytut Sportu, Warszawa, ul. Trylogii 2	z urzędu	10.07.2014 decyzja DIS/DEC-659/14/52942
21.	17-18.02.2014 DIS-K-421/21/14	Polski Związek Lekkiej Atletyki, Warszawa,ul. Mysłowicka 4	z urzędu	27.08.2014 decyzja DIS/DEC-855/14/66893
22.	17-21.02.2014 DIS-K-421/22/14	T4B Sp. z o.o., Warszawa, ul. Stanów Zjednoczonych 32 lok. U15	w związku z kontrolą DIS-K-421/153/13	nie stwierdzono uchybień
23.	24-28.02.2014 DIS-K-421/23/14	Ministerstwo Administracji i Cyfryzacji, Warszawa, ul. Królewska 27	Departament Rejestracji Zbiorów Danych Osobowych	17.09.2014 decyzja DIS/DEC-913/14/72580
24.	24-28.02.2014 DIS-K-421/24/14	Komenda Główna Żandarmerii Wojskowej, Warszawa,ul. Ostroroga 35	z urzędu	31.07.2014 decyzja DIS/DEC-765/14/59716
25.	24-28.02.2014 DIS-K-421/25/14	Mazowiecki Oddział Żandarmerii Wojskowej, Warszawa, ul. Ostroroga 35	z urzędu	nie stwierdzono uchybień
26.	03-06.03.2014 DIS-K-421/26/14	Urząd Skarbowy w Nowym Dworze Mazowieckim, Nowy Dwór Mazowiecki, ul. Legionów 7	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
27.	05-07.03.2014 DIS-K-421/27/14	Orange Polska S.A., Warszawa, Al. Jerozolimskie 160	Zespół ds. Naruszeń Danych Osobowych	nie stwierdzono uchybień
28.	10-14.03.2014 DIS-K-421/28/14	InPost Sp. z o.o., Kraków, ul. Malborska 13	z urzędu	nie stwierdzono uchybień
29.	14.03.2014 DIS-K-421/29/14	BOPOL Piotr Tokarski, Elżbieta Tokarska sp. j., Warszawa, Al. Jerozolimskie 123A lok. 419	Departament Orzecznictwa Legislacji i Skarg	07.10.2014 decyzja DIS/DEC-973/14/78316
30.	10-14.03.2014 DIS-K-421/30/14	Dayli Polska Sp. z o.o., Kraków, ul. Balicka 117	z urzędu	16.09.2014 decyzja DIS/DEC-909/14/72360
31.	10-14.03.2014 DIS-K-421/32/14	Przedsiębiorstwo Usługowo – Handlowe „Gwarancja" Rafał Szafarczyk, Mysłowice, ul. Ziętka 108	z urzędu	17.07.2014 decyzja DIS/DEC-679/14/55396
32.	12-14.03.2014 DIS-K-421/33/14	Ministerstwo Spraw Zagranicznych, Warszawa,Al. Szucha 23	z urzędu	przywrócono stan zgodny z prawem
33.	18-19.03.2014 DIS-K-421/35/14	Czesław Kędziora prowadzący działalność gospodarczą pod nazwą „P. P. H. U. BOMARD", Laski 10d, Przykona	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
34.	24-28.03.2014 DIS-K-421/36/14	Przedsiębiorstwo Handlowo – Usługowe „KREG" Sp. z o.o., Wodzisław Śl., ul. Mszańska 4C	Prokuratura Okręgowa w Gliwicach	nie stwierdzono uchybień

35.	24-28.03.2014 DIS-K-421/37/14	Starostwo Powiatowe w Gnieźnie, Gniezno, ul. Jana Pawła II 9/10	Departament Orzecznictwa Legislacji i Skarg	26.09.2014 decyzja DIS/DEC-936/14/75352
36.	25-26.03.2014 DIS-K-421/38/14	Paweł Czapliński prowadzący działalność gospodarczą pod nazwą „PPHU ARDEA", Piaseczno, ul. Warszawska 18	z urzędu	19.08.2014 decyzja DIS/DEC-821/14/64457
37.	27-28.03.2014 DIS-K-421/39/14	Halina Sobczyk prowadząca działalność gospodarczą pod nazwą „Halina Sobczyk Agencja Usługowa SOB-POL", Pruszków, ul. Sołtana 1A lok. S-3/2	z urzędu	04.07.2014 decyzja DIS/DEC-651/14/51228
38.	31.03.-03.04.2014 DIS-K-421/40/14	SP Wielospecjalistyczny Zakład Opieki Zdrowotnej MSW, Bydgoszcz, ul. Markwarta 4-6	w związku z kontrolą DIS-K-421/29/14	ustalenia wykorzystano w postępowaniu DIS-K-421/29/14
39.	31.03.-04.04.2014 DIS-K-421/41/14	Capital Service S.A., Ostrołęka, ul. Korczaka 73	Departament Orzecznictwa Legislacji i Skarg	04.07.2014 decyzja DIS/DEC-650/14/51215
40.	31.03.-04.04.2014 DIS-K-421/42/14	Urząd Miasta Płocka, Płock, Pl. Stary Rynek 1	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
41.	01-04.04.2014 DIS-K-421/43/14	e-Rachmistrz.pl Sp. z o.o., Cieszyn, ul. Limanowskiego 6	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
42.	07-09.04.2014 DIS-K-421/44/14	Urząd Gminy Rojewo, Rojewo 8	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
43.	07-11.04.2014 DIS-K-421/44/14	EMDS Sp. z o.o., Żdżarów,-Sochaczew	Departament Orzecznictwa Legislacji i Skarg	28.10.2014 decyzja DIS/DEC-1022/14/84106
44.	07-11.04.2014 DIS-K-421/46/14	Ministerstwo Pracy i Polityki Społecznej, Warszawa, ul. Nowogrodzka 1/3/5	Departament Rejestracji Zbiorów Danych Osobowych	10.09.2014 decyzja DIS/DEC-887/14/70735
45.	07-11.04.2014 DIS-K-421/47/14	Bartosz Jankowski prowadzący działalność gospodarczą pod nazwą „Bartosz Jankowski F. H. U.", Wrocław,ul. Jedności Narodowej 105	z urzędu	nie stwierdzono uchybień
46.	14-18.04.2014 DIS-K-421/49/14	Polska Grupa Pocztowa S.A., Warszawa, ul. Stanisława Augusta 75	z urzędu	nie stwierdzono uchybień
47.	22-25.04.2014 DIS-K-421/50/14	NetShops Sp. z o.o., Warszawa, ul. Żurawia 8	w związku z kontrolami DIS-K-421/170/13, DIS-K-421/173/13, DIS-K-421/175/13 i DIS-K-421/176/13	18.06.2014 decyzja DIS/DEC-577/14/47158
48.	22-25 i 28-29.04.2014 DIS-K-421/51/14	Bank Polska Kasa Opieki S.A., Warszawa,ul. Grzybowska 53/57	Departament Orzecznictwa Legislacji i Skarg	18.11.2014 wystąpienie do Komisji Nadzoru Finansowego
49.	24-25.04.2014 DIS-K-421/52/14	Ewa Gawor prowadząca działalność gospodarczą pod nazwą „GTE Ewa Gawor", Warszawa, ul. Blokowa 23B	z urzędu	nie stwierdzono uchybień

50.	28-29.04.2014 DIS-K-421/53/14	Wiktor Kaczyński prowadzący działalność gospodarczą pod nazwą „Special Service Wiktor Kaczyński", Warszawa, ul. Łabiszyńska 21	z urzędu	nie stwierdzono uchybień
51.	25 i 28.04.2014 DIS-K-421/54/14	Corrado s.c., Warszawa, Pl. Inwalidów 10	z urzędu	07.08.2014 decyzja DIS/DEC-784/14/61355
52.	29-30.04.2014 DIS-K-421/55/14	Codex Karolak, Chmiel, Stępniewska sp.j., Warszawa,ul. Górczewska 97	z urzędu	nie stwierdzono uchybień
53.	05-09.05.2014 DIS-K-421/56/14	Ministerstwo Finansów, Warszawa,ul. Świętokrzyska 12	w związku z kontrolą DIS-K-421/26/14	nie stwierdzono uchybień
54.	05-07.05.2014 DIS-K-421/57/14	Akademia Polonijna w Częstochowie, Częstochowa, ul. Pułaskiego 4/6	Okręgowa Inspekcja Pracy w Katowicach	przekazanie decyzji GI-DEC-DIS-374/05/1056 do Zespołu ds. Egzekucji Administracyjnej
55.	05-07.05.2014 DIS-K-421/58/14	BOPOL Piotr Tokarski, Elżbieta Tokarska sp.j., Warszawa, Al. Jerozolimskie 123A lok. 419	w związku z kontrolą DIS-K-421/29/14	07.10.2014 decyzja DIS/DEC-973/14/78316
56.	12-16.05.2014 DIS-K-421/59/14	Miejski Ośrodek Pomocy Społecznej w Łodzi, Łódź,ul. Piotrkowska 149	z urzędu	12.08.2014 decyzja DIS/DEC-797/14/62554
57.	12-16.05.2014 DIS-K-421/60/14	Politechnika Warszawska, Warszawa, Pl. Politechniki 1	z urzędu	25.11.2014 decyzja DIS/DEC-1117/14/92376
58.	12-16.05.2014 DIS-K-421/61/14	Uniwersytet Mikołaja Kopernika w Toruniu, Toruń, ul. Gagarina 11	z urzędu	06.11.2014 decyzja DIS/DEC-1074/14/87541
59.	12-16.05.2014 DIS-K-421/62/14	Ośrodek Pomocy Społecznej w Legionowie, Legionowo, Al. 3 Maja 28	z urzędu	nie stwierdzono uchybień
60.	19-23.05.2014 DIS-K-421/63/14	Ośrodek Pomocy Społecznej Dzielnicy Praga Południe m.st. Warszawy, Warszawa, ul. Wiatraczna 11	z urzędu	nie stwierdzono uchybień
61.	19-23.05.2014 DIS-K-421/64/14	Znany Lekarz Sp. z o.o., Warszawa, ul. Kolejowa 5/7	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
62.	19-23.05.2014 DIS-K-421/65/14	Szkoła Główna Gospodarstwa Wiejskiego, Warszawa, ul. Nowoursynowska 166	z urzędu	30.10.2014 decyzja DIS/DEC-1028/14/85023
63.	19-23.05.2014 DIS-K-421/66/14	Politechnika Lubelska, Lublin, ul. Nadbystrzycka 38D,	z urzędu	30.10.2014 decyzja DIS/DEC-1029/14/85027
64.	26-30.05.2014 DIS-K-421/67/14	Uniwersytet Warszawski, Warszawa, ul. Krakowskie Przedmieście 26/28	z urzędu	05.12.2014 decyzja DIS/DEC-1147/14/95831
65.	26-30.05.2014 DIS-K-421/68/14	Górnośląskie Towarzystwo Lotnicze S.A., Katowice, ul. Korfantego 38	w związku z kontrolą DIS-K-421/174/13	nie stwierdzono uchybień
66.	26-30.05.2014 DIS-K-421/69/14	Gminny Ośrodek Pomocy Społecznej w Jabłonnej, Jabłonna, ul. Zegrzyńska 1	z urzędu	nie stwierdzono uchybień
67.	26-30.05.2014 DIS-K-421/70/14	Ministerstwo Pracy i Polityki Społecznej, Warszawa, ul. Nowogrodzka 1/3/5	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
68.	02-06.06.2014 DIS-K-421/71/14	Gry OnLine S.A., Warszawa,ul. Zapolskiej 16A	Departament Rejestracji Zbiorów	16.12.2014 decyzja DIS/DEC-1169/14/99008

			Danych Osobowych	
69.	02-05.06.2014 DIS-K-421/72/14	Powiatowe Centrum Pomocy Rodzinie w Wołominie, Wołomin,ul. Legionów 78	z urzędu	nie stwierdzono uchybień
70.	02-06.06.2014 DIS-K-21/73/14	Prokuratura Okręgowa Warszawa – Praga, Warszawa,ul. Bródnowska 13/15	z urzędu	w toku
71.	02-06.06.2014 DIS-K-421/74/14	Prokuratura Okręgowa w Warszawie, Warszawa, ul. Chocimska 28	z urzędu	w toku
72.	09-13.06.2014 DIS-K-421/75/14	Warszawski Uniwersytet Medyczny, Warszawa, ul. Żwirki i Wigury 61	z urzędu	18.09.2014 decyzja DIS/DEC-916/14/72987
73.	09-13.06.2014 DIS-K-421/76/14	Idea Bank S.A., Warszawa, ul. Przyokopowa 33	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
74.	09-13.06.2014 DIS-K-421/77/14	Powiatowe Centrum Pomocy Rodzinie w Nowym Dworze Mazowieckim, Nowy Dwór Mazowiecki,ul. Paderewskiego 6	z urzędu	20.11.2014 decyzja DIS/DEC-1108/14/90916
75.	09-13.06.2014 DIS-K-421/78/14	Politechnika Gdańska, Gdańsk, ul. Narutowicza 11/12	z urzędu	25.11.2014 decyzja DIS/DEC-1118/14/92381
76.	09-13.06.2014 DIS-K-421/79/14	Janusz Majewski prowadzący działalność gospodarczą pod nazwą „Biuro Realizacji Inwestycji", Wałbrzych, ul. Andersa 126	Komenda Miejska Policji w Wałbrzychu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
77.	16-18 i 23.06.2014 DIS-K-421/80/14	mBank S.A., Warszawa,ul. Senatorska 18	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
78.	16-18, 20 i 23.06.2014 DIS-K-421/81/14	Instytut Hematologii i Transfuzjologii, Warszawa, ul. Indiry Ghandi 14	Departament Rejestracji Zbiorów Danych Osobowych	28.10.2014 decyzja DIS/DEC-1020/14/84091
79.	23-27.06.2014 DIS-K-421/82/14	GetBack S.A., Wrocław,ul. Powstańców Śląskich 2-4	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
80.	23-27.06.2014 DIS-K-421/83/14	Warżała i Mac System sp.j., Rzeszów,ul. Bernardyńska 10	z urzędu	nie stwierdzono uchybień
81.	23-27.06.2014 DIS-K-421/84/14	Akademia Wychowania Fizycznego, Warszawa, ul. Marymoncka 34	z urzędu	29.10.2014 decyzja DIS/DEC-1026/14/84765
82.	23.07.2014 DIS-K-421/85/14	Teresa Bukowian, Warszawa, ul. Słodowiec 8 m. 85	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
83.	07-11.07.2014 DIS-K-421/86/14	Straż Miejska w Białymstoku, Białystok,ul. Składowa 11	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
84.	07-11.07.2014 DIS-K-421/87/14	Powiatowy Urząd Pracy w Legionowie, Legionowo,ul. Andersa 11	z urzędu	nie stwierdzono uchybień
85.	14-17.07.2014 DIS-K-421/88/14	Lubuskie Zakłady Aparatów Elektrycznych „Lumel" S.A., Zielona Góra, ul. Słubicka 1	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
86.	21-25.07.2014 DIS-K-421/89/14	Seaking Poland Ltd Sp. z o.o., Czarnków,ul. Nowa 1B	Organizacja Zakładowa NSZZ Solidarność	07.11.2014 decyzja DIS/DEC-1076/14/87967

87.	21-25.07.2014 DIS-K-421/90/14	Ruch S.A., Warszawa, ul. Chłodna 52	z urzędu	nie stwierdzono uchybień
88.	21-24.07.2014 DIS-K-421/91/14	Sygnity S.A., Warszawa,Al. Jerozolimskie 180	w związku z kontrolami DIS-K-421/69/14 i DIS-K-421/77/14	nie stwierdzono uchybień
89.	21-25.07.2014 DIS-K-421/92/14	Szkoła Główna Handlowa, Warszawa,Al. Niepodległości 162	z urzędu	25.11.2014 decyzja DIS/DEC-1116/14/92372
90.	28.07-01.08.2014 DIS-K-421/93/14	Powiatowy Urząd Pracy w Wołominie, Wołomin,ul. Warszawska 5a	z urzędu	nie stwierdzono uchybień
91.	28.07-01.08.2014 DIS-K-421/94/14	Powiatowy Urząd Pracy w Łodzi, Łódź, ul. Milionowa 91	z urzędu	nie stwierdzono uchybień
92.	21-25.07.2014 DIS-K-421/95/14	Centralny Organ Techniczny (Komendant Główny Policji), Warszawa, ul. Puławska 148/150	z urzędu	31.07.2014 opinia dotycząca Krajowego Systemu Informatycznego
93.	28.07-01.08.2014 DIS-K-421/96/14	Powiatowy Urząd Pracy w Nowym Dworze Mazowieckim, Nowy Dwór Mazowiecki, ul. Słowackiego 6	z urzędu	06.11.2014 decyzja DIS/DEC-1073/14/87535
94.	28.07-01.08.2014 DIS-K-421/97/14	Stowarzyszenie Rodziców na Rzecz Pomocy Szkołom „Przyjazna Szkoła", Mysłowice, ul. Chopina 2C	Naczelnik Urzędu Skarbowego w Mysłowicach	nie stwierdzono uchybień
95.	28.07-04.08.2014 DIS-K-421/98/14	T-Mobile Polska S.A., Warszawa,ul. Marynarska 12	Departament Orzecznictwa Legislacji i Skarg	w toku
96.	28.07-04.08.2014 DIS-K-421/99/14	T-Mobile Polska S.A., Warszawa,ul. Marynarska 12	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
97.	04-08.08.2014 DIS-K-421/100/14	Vendi Servis Sp. z o.o., Łódź,- ul. Traktorowa 126	Okręgowy Inspektorat Pracy w Łodzi	04.12.2014 decyzja DIS/DEC-1145/14/95526
98.	04-08.08.2014 DIS-K-421/101/14	Hilton Foods Ltd Sp. z o.o., Tychy,ul. Strefowa 31	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
99.	11-14.08.2014 DIS-K-421/102/14	Szpital Bielański SP ZOZ, Warszawa, ul. Cegłowska 80	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
100.	18-22.08.2014 DIS-K-421/103/14	Vivid Consulting Sp. z o.o., Lublin, ul. Skromna 5	z urzędu	20.02.2015 decyzja DIS/DEC-163/15/13412
101.	18-22.08.2014 DIS-K-421/104/14	Prokuratura Okręgowa w Poznaniu, Poznań, ul. Solna 10	z urzędu	w toku
102.	18-22.08.2014 DIS-K-421/105/14	Prokuratura Okręgowa w Krakowie, Kraków, ul. Mosiężnicza 2	z urzędu	w toku
103.	18-22.08.2014 DIS-K-421/106/14	Biuro Informacji Kredytowej S.A., Warszawa, ul. Modzelewskiego 77a	Departament Orzecznictwa Legislacji i Skarg	usunięto uchybienia
104.	18-21.08.2014 DIS-K-421/107/14	Johnson & Johnson Poland Sp. z o.o., Warszawa, ul. Iłżycka 24	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
105.	25-29.08.2014 DIS-K-421/108/14	Zarząd Transportu Miejskiego w Poznaniu,Poznań, ul. Matejki	Departament Orzecznictwa	27.02.2015

		59	Legislacji i Skarg	decyzja DIS/DEC-193/15/15629
106.	25-27.08.2014 DIS-K-421/109/14	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego sp. k., Warszawa, ul. Serwituty 23	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
107.	25-27.08.2014 DIS-K-421/110/14	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego sp. k., Warszawa, ul. Serwituty 23	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
108.	25-29.08.2014 DIS-K-421/111/14	Prokuratura Generalna, Warszawa, ul. Rakowiecka 26/30	z urzędu	w toku
109.	25-29.08.2014 DIS-K-421/112/14	Mariusz Goździcki prowadzący działalność gospodarczą pod nazwą „Mariusz Goździcki Margo", Olsztyn, ul. 1 Maja 13	Prokuratura Rejonowa w Olsztynie	nie stwierdzono uchybień
110.	01-05.09.2014 DIS-K-421/113/14	PKP Intercity S.A., Warszawa,- ul. Żelazna 59A	z urzędu	2014-12-17, decyzja DIS/DEC-1183/14/99494
111.	01-05.09.2014 DIS-K-421/114/14	Przedsiębiorstwo Komunikacji Samochodowej POLONUS w Warszawie S.A., Warszawa,Al. Jerozolimskie 144	z urzędu	nie stwierdzono uchybień
112.	01-05.09.2014 DIS-K-421/115/14	Powiatowy Urząd Pracy w Żyrardowie, Żyrardów, ul. Limanowskiego 45	Prokuratura Rejonowa w Żyrardowie	2015-01-22, decyzja DIS/DEC-38/15/4870
113.	08-12.09.2014 DIS-K-421/116/14	Polska Żegluga Bałtycka S.A., Kołobrzeg,ul. Portowa 41	z urzędu	nie stwierdzono uchybień
114.	08-12.09.2014 DIS-K-421/117/14	Souter Holding Sp. z o.o., Warszawa,Al. Niepodległości 18	z urzędu	nie stwierdzono uchybień
115.	08-12.09.2014 DIS-K-421/118/14	Armatis-LC Polska Sp. z o.o., Warszawa, ul. Marynarska 15C	z urzędu	nie stwierdzono uchybień
116.	15-18.09.2014 DIS-K-421/119/14	Leroy-Merlin Sp. z o.o., Warszawa, ul. Targowa 72	Departament Orzecznictwa Legislacji i Skarg	brak przetwarzania danych osobowych w zakresie objętym kontrolą
117.	15-19.09.2014 DIS-K-421/120/14	Wydział Konsularny Ambasady RP w Oslo, Oslo,ul. Nedre Vollgate 5	z urzędu	nie stwierdzono uchybień
118.	15-19.09.2014 DIS-K-421/121/14	Wydział Konsularny Ambasady RP w Kopenhadze, Kopenhaga, ul. Richelieus Alle 12	z urzędu	nie stwierdzono uchybień
119.	15-18.09.2014 DIS-K-421/122/14	Bank Handlowy w Warszawie S.A., Warszawa, ul. Senatorska 16	Departament Orzecznictwa Legislacji i Skarg	2015-01-22, decyzja DIS/DEC-36/15/4865
120.	15-19.09.2014 DIS-K-421/123/14	Przewozy Regionalne Sp. z o.o., Warszawa, ul. Wileńska 14A	z urzędu	2015-02-04, decyzja DIS/DEC-70/15/8523
121.	18-19.09.2014 DIS-K-421/124/14	Pure Health anf Fitness Sp. z o.o., Warszawa, ul. Złota 59	z urzędu	ustalenia wykorzystano w postępowaniu DIS-K-421/7/14
122.	22-26.09.2014 DIS-K-421/125/14	Koleje Śląskie Sp. z o.o., Katowice, ul. Wita Stwosza 7	z urzędu	2014-11-07, decyzja DIS/DEC-1077/14/87970
123.	22-26.09.2014 DIS-K-421/126/14	Gmina Sokołów Podlaski, Sokołów Podlaski, ul. Wolności 44	Departament Orzecznictwa Legislacji i Skarg	2014-12-01, decyzja DIS/DEC-1132/14/94125

124.	22-26.09.2014 DIS-K-421/127/14	Kurowski G&T Sp. z o.o., Meszna, ul. Rzemieślnicza 11	Okręgowy Inspektorat Pracy	nie stwierdzono uchybień
125.	22-26.09.2014 DIS-K-421/128/14	Marek Rzeźnik prowadzący działalność gospodarczą pod nazwą „MARKPOL Transport Krajowy i Zagraniczny Marek Rzeźnik", Mielec, ul. Cyranowska 129	z urzędu	2015-01-22, decyzja DIS/DEC-37/15/4867
126.	30.09-03.10.2014 DIS-K-421/129/14	Godwin – Austin Sp. z o.o., Warszawa, Al. Jerozolimskie 81	Departament Orzecznictwa Legislacji i Skarg	08.05.2015 decyzja DIS/DEC-382/15/36383
127.	30.09-02.10.2014 DIS-K-421/130/14	Molteni Farmaceutici Polska Sp. z o.o., Kraków, ul. Obrońców Modlina 3	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
128.	29.09-02.10.2014 DIS-K-421/131/14	Wiesława Czak prowadząca działalność gospodarczą pod nazwą „Salon Muzyczny Harmoniusz Wiesława Czak", Stalowa Wola, ul. Komisji Edukacji Narodowej 13	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
129.	01-03.10.2014 DIS-K-421/132/14	Forfarm Sp. z o.o., Warszawa, ul. Chełmżyńska 219	z urzędu	nie stwierdzono uchybień
130.	06-10.10.2014 DIS-K-421/133/14	Przedsiębiorstwo Komunikacji Samochodowej w Łodzi Sp. z o.o., Łódź, ul. Smutna 28	z urzędu	2015-02-12, decyzja DIS/DEC-97/15/10356
131.	07-10.10.2014 DIS-K-421/134/14	Rafał Gnatiuk prowadzący działalność gospodarczą pod nazwą „4 Faces Rafał Gnatiuk", Lublin, ul. Witosa 3	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
132.	07-10.10.2014 DIS-K-421/135/14	Benefit Systems S.A., Warszawa, ul. Fredry 6	Departament Orzecznictwa Legislacji i Skarg	w toku
133.	07-10.10.2014 DIS-K-421/136/14	Trans Kinetik s.c. Radosław Rzepnikowski, Janusz Sadowski, Warszawa, ul. Pełczyńskiego 22a lok. 78	z urzędu	przywrócono stan zgodny z prawem
134.	13-14.10.2014 DIS-K-421/137/14	MAR-LEK Sp. z o.o. Sp. Komandytowa, Warszawa,ul. Pawła Włodkowica 2C	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
135.	13-17.10.2014 DIS-K-421/138/14	T-Mobile Polska S.A., Warszawa, ul. Marynarska 12	z urzędu	14.04.2015 decyzja DIS/DEC-321/15/29757
136.	13-17.10.2014 DIS-K-421/139/14	Kujawsko – Pomorski Transport Samochodowy S.A., Włocławek,ul. Wieniecka 39	z urzędu	20.04.2015 decyzja DIS/DEC-330/15/31147
137.	13-17.10.2014 DIS-K-421/140/14	Sąd Okręgowy we Włocławku, Włocławek, ul. Wojska Wolskiego 22	z urzędu	usunięto uchybienia
138.	13-17.10.2014 DIS-K-421/141/14	Prokuratura Apelacyjna w Warszawie, Warszawa, ul. Krakowskie Przedmieście 25	z urzędu	usunięto uchybienia
139.	20-24.10.2014 DIS-K-421/142/14	Wydział Konsularny Ambasady RP w Republice Serbii, Belgrad, ul. Kneza Milosa 38	z urzędu	nie stwierdzono uchybień

140.	20-24.10.2014 DIS-K-421/143/14	Krystian Ślebocki prowadzący działalność gospodarczą pod nazwą „Krystian Ślebocki Sand-Bus", Kutno, Wierzbnie 2E	z urzędu	2015-01-30, decyzja DIS/DEC-60/15/7229
141.	21-24.10.2014 DIS-K-421/144/14	Spółdzielczy Bank Rzemiosła i Rolnictwa, Wołomin, ul. Wąska 18	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
142.	23.10.2014 DIS-K-421/145/14	Medyk Plus Sp. z o.o., Warszawa, ul. Księcia Ziemowita 53	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
143.	23.10.2014 DIS-K-421/146/14	Phoenix Pharma Polska Sp. z o.o., Warszawa, ul. Opłotek 26	z urzędu	brak przetwarzania danych osobowych w zakresie objętym kontrolą
144.	27-28.10.2014 DIS-K-421/147/14	Solpharm Sp. z o.o., Warszawa, ul. Zwycięzców 42/93	z urzędu	2015-01-27, decyzja DIS/DEC-43/15/5960
145.	27-31.10.2014 DIS-K-421/148/14	Eurobus – Eurolines Polska Sp. z o.o., Katowice,ul. Pukowca 15	z urzędu	w toku
146.	29-31.10.2014 DIS-K-421/149/14	ACP Pharma S.A., Warszawa, - ul. Domaniewska 50	z urzędu	nie stwierdzono uchybień
147.	03-07.11.2014 DIS-K-421/150/14	TK Telekom Sp. z o.o., Warszawa, ul. Kijowska 10/12A	z urzędu	nie stwierdzono uchybień
148.	03-07.11.2014 DIS-K-421/151/14	Starostwo Powiatowe w Trzebnicy, Trzebnica, ul. Bochenka 6	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
149.	03-07.11.2014 DIS-K-421/152/14	Sąd Okręgowy w Radomiu, Radom,ul. Piłsudskiego 10	z urzędu	przywrócono stan zgodny z prawem
150.	03-07.11 i 02-05.12.2014 DIS-K-421/153/14	KBC Towarzystwo Funduszy Inwestycyjnych S.A., Warszawa,ul. Chmielna 85/87	Departament Orzecznictwa Legislacji i Skarg	25.03.2015 decyzja DIS/DEC-254/15/24557
151.	03-07.11.2014 DIS-K-421/154/14	Polski Związek Emerytów, Rencistów i Inwalidów – Oddział Rejonowy w Szczecinie, Szczecin, ul. Gryfińskiej 151	Prokuratura Rejonowa Szczecin - Prawobrzeże	w toku
152.	12-14.11.2014 DIS-K-421/155/14	Platinum Residence Sp. z o.o., Warszawa, ul. Grzybowska 61B lok. Antresola	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
153.	12-14.11.2014 DIS-K-421/156/14	GG Network S.A., Warszawa,- ul. Kamionkowska 45	Departament Orzecznictwa Legislacji i Skarg	10.03.2015 decyzja DIS/DEC-214/15/19369
154.	12.11.2014 DIS-K-421/157/14	Sanofi-Aventis Sp. z o.o., Warszawa,ul. Bonifraterska 17	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
155.	17-21.11.2014 DIS-K-421/158/14	Sąd Okręgowy w Siedlcach, Siedlce, ul. Sądowa 2	z urzędu	w toku
156.	17-20.11.2014 DIS-K-421/159/14	ENEA S.A., Poznań, ul. Góreckiej 1	w związku z kontrolą DIS-K-421/112/14	nie stwierdzono uchybień
157.	17-18.11.2014 DIS-K-421/160/14	Eli Lilly Polska Sp. z o.o., Warszawa, ul. Żwirki i Wigury 18a	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
158.	17-19.11.2014 DIS-K-421/161/14	Hotele Warszawskie Syrena Sp. z o.o., Warszawa,Pl. Konstytucji 1	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
159.	25-28.11.2014 DIS-K-421/162/14	Wydział Konsularny Ambasady RP w Republice Włoskiej,	z urzędu	nie stwierdzono uchybień

		Rzym,via Pietro Paolo Rubens 20		
160.	24-28.11.2014 DIS-K-421/163/14	Sąd Okręgowy w Krakowie, Kraków, ul. Przy Rondzie 7	z urzędu	2015-03-03, decyzja DIS/DEC-197/15/16865
161.	24-28.11.2014 DIS-K-421/164/14	Polska Grupa Farmaceutyczna S.A., Łódź, ul. Zbąszyńska 3	Departament Orzecznictwa Legislacji i Skarg	w toku
162.	01-05.12.2014 DIS-K-421/166/14	Hekon – Hotele Ekonomiczne Sp. z o.o., Łódź,Al. Piłsudskiego 11a	z urzędu	nie stwierdzono uchybień
163.	01-05.12.2014 DIS-K-421/167/14	Holding Liwa Sp. z o.o., Łódź, ul. Piotrkowska 72	z urzędu	nie stwierdzono uchybień
164.	03-05.12.2014 DIS-K-421/168/14	Abbott Laboratories Poland Sp. z o.o., Warszawa,ul. Postępu 21B	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
165.	02-05.12.2014 DIS-K-421/169/14	C.H. Robinson Polska S.A., Warszawa,Al. Jana Pawła II 29	Departament Edukacji Społecznej i Współpracy Międzynarodowej	29.04.2015 decyzja DIS/DEC-359/15/34240
166.	08-12.12.2014 DIS-K-421/170/14	Katolicka Szkoła Podstawowa im. Piotra Dunina, Chojnice, ul. Grunwaldzka 1	Departament Orzecznictwa Legislacji i Skarg	w toku
167.	08-11.12.2014 DIS-K-421/171/14	Polski Związek Emerytów, Rencistów i Inwalidów, Warszawa, Al. Jerozolimskie 30	w związku z kontrolą DIS-K-421/154/14	w toku
168.	09-12.12.2014 DIS-K-421/172/14	Wspólnota Mieszkaniowa „Pawia 2", Warszawa, ul. Bernardyńska 5	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
169.	08-12.12.2014 DIS-K-421/173/14	Powszechny Zakład Ubezpieczeń S.A., Warszawa, Al. Jana Pawła II 24	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
170.	08-12.12.2014 DIS-K-421/174/14	Powszechny Zakład Ubezpieczeń na Życie S.A., Warszawa, Al. Jana Pawła II 24	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
171.	11-12.12.2014 DIS-K-421/175/14	AstraZeneca Pharma Poland Sp. z o.o., Warszawa, ul. Postępu 18	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
172.	10-12.12.2014 DIS-K-176/14	Amgen Sp. z o.o., Warszawa, ul. Domaniewska 50	W związku z kontrolą DIS-K-421/164/14	nie stwierdzono uchybień
173.	15-19.12.2014 DIS-K-421/177/14	Szafa.pl Sp. z o.o., Rzeszów, ul. Laurowa 18/1	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa, Legislacji i Skarg
174.	15-19.12.2014 DIS-K-421/178/14	Rafał Celi, prowadzący działalność gospodarczą pod nazwą „Euroadres Polska Rafał Celi", Warszawa, ul. Batorego 18	W związku z kontrolą DIS-K-421/129/14	12.05.2014 decyzja DIS/DEC-390/15/37284
175.	15-19.12.2014 DIS-K-421/179/14	Sąd Apelacyjny w Warszawie, Warszawa,Pl. Krasińskich 2/4/6	z urzędu	w toku

Załącznik nr 3

Wykaz orzeczeń wydanych w 2014 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.	03.01.2014 r. II SA/Wa 1506/13	DOLiS/POST-315/12/53547	Skarga na postanowienie w przedmiocie zwrotu pisma z tytułu nieuiszczenia opłaty skarbowej	Postanowienie WSA o odmowie przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika.
2.	08.01.2014 r. II SA/Wa 935/13	DOLiS/DEC-254/13/ 13267,13270,13271	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi.
3.	10.01.2014 r. II SA/Wa 1648/13	DOLiS/DEC-625/13/37430,37431	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.
4.	15.01.2014 r. II SA/Wa 1082/13	DOLiS/DEC-376/13/20434,20436	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji w części objętej wnioskami o ponowne rozpatrzenie sprawy oraz określenie, że nie podlega wykonaniu w całości.
5.	16.01.2014 r. II SA/Wa 1288/13	DOLiS/DEC-595/13/33662,33665,33668	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi.
6.	16.01.2014 r. II SA/Wa 919/13	DOLiS/DEC-315/13/17458,17461	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi.
7.	17.01.2014 r. II SA/Wa 974/13	DOLiS/DEC-313/13/17462,17465,17467	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi.
8.	17.01.2014 r. II SA/Wa 1465/13	GI-DOLiS-430/254/07	Skarga o wznowienie postępowania sądowego zakończonego wyrokiem WSA w Warszawie z dnia 22.12.2009 r. o sygn. akt II SA/Wa 710/09	Postanowienie WSA – odrzucenie skargi w sprawie o wznowienie postępowania.
9.	23.01.2014 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820,43822-	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – oddalenie wniosku o wyłączenie sędziego.
10.	23.01.2014 r. II SA/Wa 1664/13	DOLiS/DEC-589/13/33413, 33421	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie wniosku o przywrócenie terminu do wniesienia skargi.

11.	23.01.2014 r. I OZ 15/14	DOLiS/POST-315/12/53547	Skarga na postanowienie w przedmiocie zwrotu pisma z tytułu nieuiszczenia opłaty skarbowej	Postanowienie NSA – oddalono zażalenie na postanowienie WSA w Warszawie z dnia 29.11.2013 r., sygn. akt II SA/Wa 1506/13 o odmowie przyznania prawa pomocy w zakresie całkowitym obejmującym zwolnienie od kosztów sądowych i ustanowienie adwokata lub radcy prawnego.
12.	23.01.2014 r. I OZ 14/14	DOLiS/POST-315/12/53547	Skarga na postanowienie w przedmiocie zwrotu pisma z tytułu nieuiszczenia opłaty skarbowej	Postanowienie NSA – oddalono zażalenie na postanowienie WSA w Warszawie z dnia 29.11.2013 r., sygn. akt II SA/Wa 1506/13 o odmowie przyznania prawa pomocy w zakresie całkowitym obejmującym zwolnienie od kosztów sądowych i ustanowienie adwokata lub radcy prawnego.
13.	23.01.2014 r. I OZ 13/14	DOLiS/POST-315/12/53547	Skarga na postanowienie w przedmiocie zwrotu pisma z tytułu nieuiszczenia opłaty skarbowej	Postanowienie NSA – oddalono zażalenie na postanowienie WSA w Warszawie z dnia 29.11.2013 r., sygn. akt II SA/Wa 1506/13 o odmowie przyznania prawa pomocy w zakresie całkowitym obejmującym zwolnienie od kosztów sądowych i ustanowienie adwokata lub radcy prawnego.
14.	24.01.2014 r. II SA/Wa 1537/13	DOLiS/DEC-828/13/49462,49465	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o odmowie przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika.
15.	27.01.2014 r. II SAB/Wa 537/13	DOLiS-440-102/13	Skarga na bezczynność organu	Wyrok WSA stwierdzający, iż bezczynność miała miejsce z rażącym naruszeniem prawa, wymierzający grzywnę w wysokości 1000 zł oraz w pozostałym zakresie umarzający postępowanie.
16.	27.01.2014 r. II SA/Wa 2112/13	DOLiS/DEC-852/11/48406,48408	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.
17.	27.01.2014 r. II SA/Wa 2104/13	DOLiS/DEC-989/11/56229,56238	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że nie podlegają wykonaniu w całośc.i
18.	27.01.2014 r. II SAB/Wa 693/13	DOLiS-440-1492/12	Skarga na przewlekłe prowadzenie postępowania przez GIODO	Postanowienie WSA – odrzucenie skargi.
19.	28.01.2014 r. II SA/Wa 1366/13	DOLiS/DEC-520/13/29452,29456	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.
20.	28.01.2014 r.	DOLiS/DEC-	Skarga na decyzję w przedmiocie	Postanowienie WSA o przyznaniu

	II SA/Wa 1557/13	257/12/19946,19951	ochrony danych osobowych	środków budżetowych WSA w Warszawie tytułem nieopłaconej pomocy prawnej udzielonej z urzędu.
21.	29.01.2014 r. I OSK 145/14	DOLiS/DEC-1129/10/37954,37958	Skarga kasacyjna od postanowienia WSA z dn. 22.10.2013 r. w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	Postanowienie NSA – oddalenie skargi kasacyjnej na postanowienie WSA w Warszawie z dnia 22.10.2013 r. sygn. akt II SA/Wa 1249/13 o odrzuceniu skargi Komendanta.
22.	29.01.2014 r. II SA/Wa 1819/13	DOLiS/DEC-777/13/47061,47062	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.
23.	29.01.2014 r. II SAB/Wa 765/13	DOLiS-440-785/13	Skarga na bezczynność organu	Postanowienie WSA – umorzenie postępowania
24.	31.01.2014 r. I OSK 2460/13	DOLiS-440-1162/12	Skarga kasacyjna GIODO od wyroku WSA z dn. 10.06.2013 r. w sprawie skargi na przewlekłość postępowania	Wyrok NSA – oddalający skargę kasacyjną GIODO od wyroku WSA w Warszawie z dnia 10.06.2013 r. sygn. akt II SAB/Wa 145/13.
25.	03.02.2014 r. II SAB/Wa 650/13	DOLiS-440-116/11	Skarga na bezczynność organu	Wyrok WSA stwierdzający, iż przewlekłość postępowania miała miejsce z rażącym naruszeniem prawa i w pozostałym zakresie umarzający postępowanie.
26.	03.02.2014 r. II SA/Wa 1909/13	DOLiS/DEC-828/13/49462,49465	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji oraz określenie, że nie podlega wykonaniu w całości.
27.	04.02.2014 r. II SA/Wa 293/13	DOLiS/DEC-1255/12/77408,77409	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi.
28.	04.02.2014 r. II SA/Wa 2227/13	DOLiS/DEC-1081/11/63114,63126	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.
29.	05.02.2014 r. II SA/Wa 1150/13	DOLiS/DEC-436/13/23569,23570	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji oraz określenie, że nie podlega wykonaniu w całości.
30.	06.02.2014 r. II SA/Wa 144/14	DIS-DEC-1234/13/81208	Niezastosowanie środków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych osobowych.	Odrzucenie skargi
31.	07.02.2014 r. II SA/Wa 2093/13	DOLiS/DEC-857/13/53258,53266	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie częściowym obejmującym ustanowienie radcy prawnego.
32.	10.02.2014 r. II SA/Wa 125/14	DIS/DEC-1190/13/76126	Niedopełnienie obowiązku informacyjnego	Wstrzymanie wykonania decyzji
33.	10.02.2014 r. II SAB/Wa 566/13	DOLiS-440-981/12	Skarga na bezczynność organu w przedmiocie rozpatrywania skargi	Wyrok WSA stwierdzający, iż bezczynność miała miejsce z rażącym naruszeniem prawa,

				wymierzający grzywnę w wysokości 1000 zł oraz w pozostałym zakresie umarzający postępowanie.
34.	13.02.2014 r. I OSK 1982/12	DOLiS/DEC-825/11/45756, 45759	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 18.04.2012 r. sygn. akt II SA/Wa 2710/11 w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 18.04.2012 r. sygn. akt II SA/Wa 2710/11 i przekazujący sprawę do ponownego rozpoznania przez WSA.
35.	13.02.2014 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820,438 22-	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA odmawiające zawieszenia postępowania.
36.	13.02.2014 r. I OSK 1641/12	DOLiS/DEC-712/11/49238,402 52	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 08.03.2012 r. w sprawie skargi na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 8.03.2012 r. sygn. akt II SA/Wa 2464/11.
37.	13.02.2014 r. I OSK 2436/12	DOLiS/DEC-55/12/3326,3331	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 06.06.2012 r. w sprawie skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 06.06.2012 r. sygn. akt II SA/Wa 453/12.
38.	13.02.2014 r. I OSK 1806/12	DOLiS/POST-215/11/44888, 44893	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 1.03.2012 r. sygn. akt II SA/Wa 2661/11 w sprawie ze skargi na postanowienie w przedmiocie odmowy wydania kserokopii akt sprawy	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 1.03.2012 r. sygn. akt II SA/Wa 2661/11.
39.	13.02.2014 r. I OSK 1772/12	DOLiS/POST-232/11/50704,507 12,80718,50714,50 719	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 19.04.2012 r. w sprawie ze skargi na postanowienie w przedmiocie odmowy wydania kserokopii akt sprawy	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 19.04.2012 r. sygn. akt II SA/Wa 2745/11 i przekazujący sprawę do ponownego rozpoznania przez WSA.
40.	13.02.2014 r. I OSK 1771/12	DOLiS/DEC-507/11/29785,297 84,29782,29783,29 786	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 19.04.2012 r. w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA uchylający wyrok WSA w Warszawie z dnia 19.04.2012 r. sygn. akt II SA/Wa 2590/11 i przekazujący sprawę do ponownego rozpoznania przez WSA.
41.	14.02.2014 r. II SAB/Wa 381/13	DOLiS-035-4067/12	Skarga na bezczynność organu w przedmiocie rozpoznania wniosku	Wyrok WSA – oddalenie skargi i przyznanie ze środków budżetowych WSA w Warszawie na rzecz adwokata kwoty tytułem nieopłaconej pomocy prawnej udzielonej z urzędu.
42.	14.02.2014 r. II SA/Wa 2013/13	DOLiS/POST-274/13/58491	Skarga na postanowienie w przedmiocie zwrotu skargi wobec nieuiszczenia opłaty skarbowej	Postanowienie WSA o przyznaniu prawa pomocy w zakresie obejmującym zwolnienie od kosztów sądowych oraz ustanowienie radcy prawnego lub adwokata.
43.	18.02.2014 r.	DOLiS/POST-	Skarga na postanowienie w	Postanowienie NSA – oddalenie

	I OZ 100/14	315/12/53547	przedmiocie zwrotu pisma z uwagi na nieuiszczenie opłaty skarbowej	zażalenia na postanowienie WSA w Warszawie z dnia 3.01.2014 r., sygn. akt II SA/Wa 1506/13.
44.	19.02.2014 r. I OSK 1843/13	DOLiS-440-200/07	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 15.11.2010 r. sygn. akt. II SA/Wa 1477/10 w sprawie skargi o wymierzenie grzywny z tytułu niewykonania wyroku WSA w Warszawie z dnia 15.11.2010 r. sygn. akt. II SA/Wa 1477/10	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 15.11.2010 r. sygn. akt. II SA/Wa 1477/10 i przekazujący sprawę do ponownego rozpoznania przez WSA.
45.	19.02.2014 r. II SA/Wa 1945/13	DOLiS/DEC-932/13/57589,57593,57596,57622	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
46.	20.02.2014 r. II SA/Wa 2125/13	DOLiS/DEC-1056/13/63947,63953	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
47.	21.02.2014r. I OSK 2445/12	DIS/DEC-103/12/7510	Niewyznaczenie administratora bezpieczeństwa informacji.	Oddalenie skargi kasacyjnej
48.	21.02.2014 r. I OSK 2324/12	DOLiS/DEC-200/12/15293,15306	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 18.06.2012 r. w sprawie skargi na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 18.06.2012 r. sygn. akt II SA/Wa 842/12 i przekazujący sprawę do ponownego rozpoznania przez WSA.
49.	21.02.2014 r. I OSK 2068/12	DOLiS/DEC-15/12/901,906	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 04.06.2012 r. w sprawie skargi na decyzję w przedmiocie obowiązku informacyjnego odnośnie przetwarzania danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 04.06.2012 r. sygn. akt II SA/Wa 289/12 i przekazujący sprawę do ponownego rozpoznania przez WSA.
50.	21.02.2014 r. I OSK 2056/12	DOLiS/DEC-870/11/49743,49751	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 20.03.2012 r. w sprawie skargi na decyzję w przedmiocie umorzenia postępowania administracyjnego	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 20.03.2012 r. sygn. akt II SA/Wa 2493/11 i przekazujący sprawę do ponownego rozpoznania przez WSA.
51.	21.02.2014 r. I OSK 2331/12	DOLiS/DEC-785/11/43105,43113	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 07.05.2012 r. w sprawie skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej.
52.	21.02.2014 r. I OSK 2463/12	DOLiS/DEC-806/11/44578, 44587	Skarga kasacyjny od wyroku WSA w Warszawie z dnia 31.05.2012 r. w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
53.	21.02.2014 r. I OSK 2445/12	DOLiS/DEC-	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 05.07.2012 r. w sprawie skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej
54.	24.02.2014 r. II SA/Wa 2249/13	DOLiS/POST-291/13/63537	Skarga na postanowienie w przedmiocie w przedmiocie	Wyrok WSA uchylający zaskarżone postanowienie oraz

			odmowy wszczęcia postępowania w sprawie przetwarzania danych osobowych	postanowienie je poprzedzające i stwierdzenie, że nie podlega ono wykonaniu w całości.
55.	25.02.2014 r. II SA/Wa 2334/13	DOLiS/DEC-1060/12/66556,66559	Skarga na decyzję w przedmiocie umorzenia postępowania	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
56.	26.02.2014 r. II SA/Wa 2312/13	DOLiS/DEC-127/12/9056,9080	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
57.	27.02.2014 r. II SA/Wa 93/14	DOLiS-440-1293/13	Skarga na pismo w przedmiocie wezwania do uzupełnienia braków formalnych podania i uiszczenia opłaty skarbowej	Postanowienie WSA – odrzucenie skargi
58.	04.03.2014 r. II SA/Wa 2393/13	DIS/DEC-1115/13/69420	Niezastosowanie środków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych osobowych, niezgłoszenie do rejestracji zbioru danych osobowych, niezawarcie w dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym wszystkich wymaganych elementów	Odmowa wstrzymania wykonania decyzji
59.	04.03.2014 r. II SA/Wa 2393/13	DIS/DEC-1115/13/69420	Niezastosowanie środków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych osobowych, niezgłoszenie do rejestracji zbioru danych osobowych, niezawarcie w dokumentacji stanowiącej politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym wszystkich wymaganych elementów	Oddalenie skargi
60.	04.03.2014 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820,43822	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – przywrócenie terminu do wniesienia zażalenia
61.	04.03.2014 r. II SA/Wa 974/13	DOLiS/DEC-313/13/17462,17465,17467	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Postanowienie WSA - przyznanie wynagrodzenia za zastępstwo prawne wykonane na zasadzie prawa pomocy.
62.	04.03.2014 r. II SA/Wa 1568/13	DOLiS/DEC-609/13/35406,35422,35430,35434,35433,35448,35451,24455,35458,3461,35465,35470	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - przyznanie kosztów nieopłaconej pomocy prawnej udzielonej z urzędu.
63.	05.03.2014 r. II SA/Wa 1999/13	DOLiS/POST-293/13/65257,652	Skarga na postanowienie w przedmiocie sprostowania	Postanowienie WSA – odmowa przyznania prawa pomocy w

		59	omyłki pisarskiej	zakresie zwolnienia od kosztów sądowych.
64.	05.03.2014 r. II SA/Wa 1648/13	DOLiS/DEC-625/13/37430,37431	Skarga na decyzję	Postanowienie WSA - przyznanie prawa pomocy w zakresie całkowitym obejmującym ustanowienie adwokata oraz zwolnienie od kosztów sądowych.
65.	06.03.2014 r, II SA/Wa 2413/13	GI-DOLiS-430/254/07	Skarga w przedmiocie skargi o wznowienie postępowania w sprawie zakończonej wyrokiem WSA w Warszawie z 14 grudnia 2011 r. sygn. akt II SA/Wa 1582/11	Postanowienie WSA – przywrócenie terminu do wniesienia skargi
66.	06.03.2014 r. I OSK 407/14	DOLiS/DEC-117/13/8319,8320	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Postanowienie NSA o wstrzymaniu wykonania zaskarżonej decyzji
67.	11.03.2014 r. II SA/Wa 14/14	DOLiS/DEC-1066/12/66593,66597	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
68.	13.03.2014 r. II SA/Wa 1988/13	DOLiS/DEC-884/13/51110,51096	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
69.	13.03.2014 r. II SA/Wa 1696/13	DOLiS/DEC-656/13/38658,38666	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
70.	14.03.2014 r. II SA/Wa 376/14	DOLiS/POST-6/14/882	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Postanowienie WSA - przyznanie prawa pomocy w zakresie obejmującym zwolnienie od kosztów sądowych oraz ustanowienie adwokata.
71.	17.03.2014 r. II SA/Wa 1338/13	DOLiS/DEC-519/13/29101,29106	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
72.	18.03.2014 r. I OZ 183/14	DOliS/DEC-598/13/34106,34107,34108	Skarga na decyzję w przedmiocie przekazania danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 20.12.2013 r. sygn. akt II SA/Wa 1333/13 o odmowie przywrócenia terminu do usunięcia braków formalnych skargi.
73.	21.03.2014 r. II SA/Wa 2275/13	DOLiS/DEC-1085/13/66500,66502,66507	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
74.	24.03.2014 r. II SA/Wa 1545/13	DOLiS/POST-144/13/33396,33399,33416	Skarga na postanowienie w przedmiocie odmowy wydania uwierzytelnionych odpisów dokumentów	Wyrok WSA – oddalenie skargi
75.	27.03.2014 r. II SAB/Wa 559/13	DOLiS-440-937/12	Skarga na bezczynność organu w przedmiocie skargi na udostępnienie danych osobowych	Wyrok WSA – oddalenie skargi
76.	04.04.2014 r. II SA/Wa 174/14	DOLiS/DEC-1349/13/86406,86414,86421	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Postanowienie WSA - przyznanie prawa pomocy w zakresie całkowitym obejmującym ustanowienie adwokata oraz

				zwolnienie od kosztów sądowych.
77.	09.04.2014 r. I OZ 266/14	DOLiS/DEC-589/13/33413,33421	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 23.01.2014 r., sygn. akt II SA/Wa 1664/13.
78.	10.04.2014 r. II SA/Wa 1401/13	DOLiS/DEC-657/13/38688,38692	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
79.	14.04.2014 r. II SA/Wa 2093/13	DOLiS/DEC-	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Wyrok WSA – oddalenie skargi
80.	16.04.2014 r. II SA/Wa 2661/11	DOLiS/POST-215/11/44888, 44893	Skarga na postanowienie w przedmiocie odmowy wydania kserokopii akt sprawy	Postanowienie WSA - przyznanie kosztów nieopłaconej pomocy prawnej udzielonej z urzędu.
81.	18.04.2014 r. I OSK 1460/13	DOLiS/DEC-652/12/43574,43575	Skarga kasacyjna od wyroku WSA z dnia 13.02.2013 r. w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 13.02.2013 r. sygn. akt II SA/Wa 1654/12.
82.	18.04.2014 r. I OSK 2789/12	DOLiS/DEC-197/12/15277,15281	Skarga kasacyjna od wyroku WSA z dnia 26.07.2012 r. w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 26.07.2012 r. sygn. akt II SA/Wa 892/12.
83.	22.04.2014 r. II SA/Wa 570/14	DOLiS/DEC-25/14/4154,4156	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
84.	22.04.2014 r. II SA/Wa 569/14	DOLiS/DEC-24/14/4152,4153	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
85.	24.04.2014 r. II SA/Wa 125/14	DIS/DEC-1190/13/76126	Niedopełnienie obowiązku informacyjnego	Uchylenie zaskarżonej decyzji
86.	24.04.2014 r. II SA/Wa 1648/13	DOLiS/DEC-625/13/37430,37431	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odmowa przyznania pełnomocnikowi wynagrodzenia za zastępstwo prawne.
87.	24.04.2014 r. II SA/Wa 2383/11	DOLiS/DEC-785/11/43105,43113	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Postanowienie WSA - przyznanie kosztów nieopłaconej pomocy prawnej udzielonej z urzędu.
88.	25.04.2014 r. II SA/Wa 30/14	DIS/DEC-1179/13/75064	Niedopełnienie obowiązku informacyjnego, niezapewnienie, aby dostęp do danych przetwarzanych z wykorzystaniem systemu informatycznego możliwy był wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia	Oddalenie skargi
89.	25.04.2014 r. II SA/Wa 30/14	DOLiS/DEC-313/14/25430,25431	Skarga na decyzję w przedmiocie nakazu usunięcia uchybień w procesie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
90.	28.04.2014 r. II SA/Wa 389/14	DOLiS/DEC-5/14/943,948	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji.
91.	05.05.2014 r.	DOLiS/DEC-	Skarga na decyzję w przedmiocie	Postanowienie WSA –

	II SA/Wa 644/14	64/14/7471,7476	ochrony danych osobowych	wstrzymanie wykonania zaskarżonej decyzji w części obejmującej nakaz udostępnienia danych osobowych.
92.	06.05.2014 r. II SA/Wa 1999/13	DOLiS/POST-293/13/65257,65259	Skarga na postanowienie w przedmiocie sprostowania omyłki pisarskiej	Postanowienie WSA – odrzucenie skargi
93.	06.05.2014 r. I OSK 953/14	DOLiS/DEC-828/13/49462,49465,	Skarga kasacyjna od postanowienia WSA z dnia 03.10.2013 r. w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA – oddalenie skargi kasacyjnej od postanowienia WSA w Warszawie z dnia 3.10.2013 r., sygn. akt II SA/Wa 1537/13.
94.	07.05.2014 r. II SA/Wa 375/14	DOLiS/DEC-21/14/3779,3818,3824	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku o kontrolę przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
95.	07.05.2014 r. II SAB/Wa 96/14	DOLiS-440-1046/09	Skarga na przewlekłość organu w przedmiocie prowadzenia postępowania w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający przewlekłość postępowania administracyjnego i że przewlekłość postępowania miała charakter rażący.
96.	14.05.2014 r. II SAB/Wa 163/14	GIODO-067-4/13	Skarga na bezczynność organu w przedmiocie rozpoznania wniosku o udostępnienie informacji publicznej	Postanowienie WSA - odrzucenie skargi
97.	14.05.2014 r. II SAB/Wa 8/14	DOLiS-440-1530/12	Skarga na przewlekłość organu w przedmiocie rozpoznania wniosku o ponowne rozpatrzenie sprawy ze skargi na przetwarzanie danych osobowych	Postanowienie WSA - odrzucenie skargi
98.	14.05.2014 r. I OSK 176/13	DOLiS/DEC-87/12/6486,6502,6505	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 17.10.2012 r. o sygn. akt II SA/Wa 600/12 ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA – umorzenie postępowania z art. 161 Ppsa
99.	15.05.2014 r. II SAB/Wa 174/14	DOLiS-440-857/12	Skarga na bezczynność GIODO w przedmiocie rozpoznania wniosku o ponowne rozpatrzenie sprawy	Postanowienie WSA – umorzenie postępowania z art. 161 Ppsa
100.	19.05.2014 r. II SA/Wa 1648/13	DOLiS/DEC-625/13/37430,37431	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA - przyznanie kosztów nieopłaconej pomocy prawnej udzielonej z urzędu.
101.	20.05.2014 r. II SA/Wa 2013/13	DOLiS/POST-274/13/58491	Skarga na postanowienie w przedmiocie zwrotu skargi wobec nieuiszczenia w wyznaczonym terminie należności tytułem opłaty skarbowej	Wyrok WSA – oddalenie skargi
102.	22.05.2014 r. I OSK 1982/12	DOLiS/DEC-825/11/45756,45759	Skarga kasacyjna GIODO od wyroku WSA z dnia 18.04.2012 r. sygn. akt II SA/Wa 2710/11 w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	Postanowienie NSA odmawiające wykładni wyroku

103.	22.05.2014 r. II SA/Wa 2093/13	DOLiS/DEC-857/13/53258,53266	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA - przyznanie prawa pomocy w zakresie obejmującym zwolnienie od kosztów sądowych.
104.	22.05.2014 r. II SA/Wa 507/14	DOLiS/DEC-825/11/45756,45759	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skargi
105.	27.05.2014 r. II SA/Wa 514/14	DOLiS/DEC-507/11/29785,29784,29782,29783,29786	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
106.	27.05.2014 r. II SA/Wa 457/14	DOLiS/DEC-2/14/654,661	Skarga na decyzję w przedmiocie przetwarzania danych	Postanowienie WSA – odrzucenie skargi
107.	27.05.2014 r. II SA/Wa 515/14	DOLiS/POST-207/11/44269, 44276, 44277, 44279, 44281	Skarga na postanowienie w przedmiocie odmowy wydania kserokopii akt sprawy	Wyrok WSA – oddalenie skargi
108.	04.06.2014 r. II SA/Wa 2413/13	Dot. DOLiS-440-429/10	Skarga w przedmiocie wznowienia postępowania w sprawie zakończonej wyrokiem WSA w Warszawie z dnia 14.12.2011 r. sygn. akt II SA/Wa 1582/11	Wyrok WSA – oddalono skargę o wznowienie postępowania.
109.	05.06.2014 r. II SA/Wa 727/14	DOLiS/DEC-171/14/14199,14202	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
110.	09.06.2014 r. II SA/Wa 2152/13	DOLiS/DEC-928/13/57143,57161,57173	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Wyrok WSA – oddalenie skargi
111.	16.06.2014 r. II SAB/Wa 278/14	DOLiS-440-615/11	Skarga na bezczynność w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
112.	17.06.2014 r. II SA/Wa 791/14	DOLiS/DEC-186/14/17111,17117	Skarga na decyzję w przedmiocie przetwarzania danych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
113.	17.06.2014 r. I OZ 459/14	DOLiS/DEC-5/14/943,948	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 28.04.2014 r., sygn. akt II SA/Wa 389/14.
114.	24.06.2014 r. II SAB/Wa 329/14	Dot. DOLiS-440-150/11	Skarga na bezczynność i przewlekłe prowadzenia postępowania przez organ w przedmiocie wydania decyzji	Postanowienie WSA – odrzucenie skargi
115.	24.06.2014 r. II SA/Wa 568/14	DOLiS/DEC-65/14/7512,7519	Skarga na decyzję w przedmiocie nakazania przywrócenia stanu zgodnego z prawem	Postanowienie WSA – odrzucenie skargi
116.	26.06.2014 r. II SA/Wa 2394/13	DOLiS/DEC-1186/13/75909,75916	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Wyrok WSA – oddalenie skargi
117.	26.06.2014 r. II SA/Wa 726/14	DOLiS/DEC-171/14/14199,14202	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie skargi
118.	27.06.2014 r. II SA/Wa 643/14	DOLiS/DEC-200/12/15293,15306	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja

				nie podlega wykonaniu w całości.
119.	27.06.2014 r. II SA/Wa 748/14	DOLiS/DEC-870/11/49743,49751	Skarga na decyzję w przedmiocie umorzenia postępowania administracyjnego	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
120.	02.07.2014 r. II SA/Wa 749/14	DOLiS/DEC-15/12/901,906	Skarga na decyzję w przedmiocie obowiązku informacyjnego odnośnie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
121.	02.07.2014 r. II SA/Wa 675/14	DOLiS-440-200/07	Skarga o wymierzenie GIODO grzywny z tytułu niewykonania wyroku WSA w Warszawie z dnia 15.11.2010 r. sygn. akt II SA/Wa 1477/10	Wyrok WSA - wymierzenie GIODO grzywny z tytułu niewykonania wyroku WSA w Warszawie z dnia 15.11.2010 r. sygn. akt II SA/Wa 1477/10 1. w wysokości 5000,00 zł (pięć tysięcy złotych), oraz stwierdzenie, że prowadzenie postępowania przez organ po ww. wyroku miało miejsce z rażącym naruszeniem prawa.
122.	02.07.2014 r. II SA/Wa 291/14	DOLiS/DEC-1351/13/86510,86516,86521,86526	Skarga na decyzję w przedmiocie przetwarzania danych	Wyrok WSA – oddalenie skargi
123.	09.07.2014 r. II SA/Wa 841/14	DOLiS/DEC-153/14/13124,13128,13132,13134	Skarga na decyzję w przedmiocie odmowy uwzględnienia skargi na przetwarzanie danych osobowych	Postanowienie WSA – uchylenie zarządzenia Przewodniczącego Wydziału II z dnia 30.05.2014 r. o wezwaniu do uiszczenia wpisu sądowego.
124.	10.07.2014 r. II SAB/Wa 276/14	DOLiS-440-1440/13	Skarga na bezczynność organu w przedmiocie rozpoznania skargi dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
125.	16.07.2014 r. II SA/Wa 930/14	DOLiS/DEC-313/14/25430,25431	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
126.	18.07.2014 r. II SA/Wa 570/14	DOLiS/DEC-25/14/4154,4156	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
127.	18.07.2014 r. II SA/Wa 569/14	DOLiS/DEC-24/14/4152,4153	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
128.	22.07.2014 r. II SA/Wa 1506/13	DOLiS/POST-315/12/53547	Skarga na postanowienie w przedmiocie zwrotu pisma z uwagi na nieuiszczenie opłaty skarbowej	Postanowienie WSA – odrzucenie skargi
129.	24.07.2014 r. II SAB/Wa 391/14	DOLiS-440-167/14	Skarga na przewlekłość prowadzenia postępowania przez organ w przedmiocie ochrony danych osobowych	Postanowienie WSA - przyznanie prawa pomocy w zakresie całkowitym obejmującym ustanowienie adwokata lub radcy prawnego oraz zwolnienie od kosztów sądowych.
130.	24.07.2014 r. II SA/Wa 2093/13	DOLiS/DEC-857/13/53258,53266	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA – odrzucenie skargi kasacyjnej
131.	24.07.2014 r. II SAB/Wa 300/14	DOLiS-440-187/13	Skarga na bezczynność organu w przedmiocie rozpatrzenia skargi w sprawie przetwarzania danych	Postanowienie WSA – odrzucenie skargi

			osobowych	
132.	25.07.2014 r. II SA/Wa 389/14	DOLiS/DEC-5/14/943,948	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA - wstrzymanie wykonania zaskarżonej decyzji
133.	31.07.2014 r. I OZ 608/14	DOLiS/DEC-727/13/43820,43822-	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 20.01.2014 r., sygn. akt II SA/Wa 1789/13.
134.	31.07.2014 r. I OSK 742/13	DOLiS/DEC-418/12/29729,29736	Skarga kasacyjna GIODO od wyroku WSA z dn.05.12.2012 r. w sprawie skargi na decyzję w przedmiocie ochrony danych osobowych	Wyrok NSA – oddalenie skarg kasacyjnych GIODO i Szefa Kancelarii Sejmu od wyroku WSA w Warszawie z dnia 5.12.2012 r. sygn. akt II SA/Wa 1145/12.
135.	31.07.2014 r. I OSK 2846/12	DOLiS-440-200/07	Skarga w przedmiocie odmowy stwierdzenia nieważności	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 17.07.2012 r. sygn. akt II SA/Wa 832/12.
136.	06.08.2014 r. II SA/Wa 1242/14	DOLiS/DEC-419/14/33391,33397	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA odmawiające wstrzymania wykonania zaskarżonej decyzji
137.	12.08.2014 r. II SA/Wa 1002/14	DOLiS/DEC-302/14/24569,24572,24577,24581,24583	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – odrzucenie zażalenia na zarządzenie Przewodniczącej Wydziału II WSA w Warszawie z dnia 23.06.2014 r., sygn. akt II SA/Wa 1002/14.
138.	20.08.2014 r. II SA/Wa 1025/14	DOLiS-440-167/14	Skarga na pismo w przedmiocie żądania oryginału zaświadczenia	Postanowienie WSA – odrzucenie skargi
139.	20.08.2014 r. II SAB/Wa 392/14	Dot. DOLiS-440-167/14	Skarga na niezałatwienie przez GIODO w terminie sprawy dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
140.	21.08.2014 r. II SA/Wa 389/14	DOLiS/DEC-5/14/943,948	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
141.	29.08.2014 r. II SA/Wa 847/14	DOLiS/DEC-228/14/18930,18935	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA odmawiające wstrzymania wykonania zaskarżonej decyzji.
142.	29.08.2014 r. II SA/Wa 791/14	DOLiS/DEC-186/14/14111,14117	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie zażalenia na postanowienie WSA w Warszawie z dnia 17.06.2014 r.
143.	29.08.2014 r. II SA/Wa 848/14	DOLiS/DEC-228/14/18930,18935	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
144.	03.09.2014 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820,43822-	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie zażalenia na postanowienie z 13.02.2014 r. o sygn. akt II SA/Wa 1789/13 WSA w Warszawie o odmowie zawieszenia postępowania sądowego.
145.	05.09.2014 r. II SA/Wa 790/14	DOLiS/DEC-142/14/12402,12408,12411	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika.

146.	15.09.2014 r. II SA/Wa 2394/13	DOLiS/DEC-1186/13/75909,75916	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych.
147.	19.09.2014 r. II SAB 208/14	DOLiS-440-981/12	Skarga na bezczynność organu w przedmiocie rozpoznania wniosku o ponowne rozpatrzenie sprawy zakończonej decyzją o odmowie uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż bezczynność nie miała miejsca z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie.
148.	23.09.2014 r. II SA/Wa 174/14	DOLiS/DEC-1349/13/86406,86414,86421	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Wyrok WSA – oddalenie skargi
149.	23.09.2014 r. II SA/Wa 376/14	DOLiS/POST-6/14/882	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Wyrok WSA – oddalenie skargi
150.	23.09.2014 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820,43822-	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA o wyłączeniu sędziego
151.	23.09.2014 r. II SA/Wa 998/14	DOLiS/DEC-299/14/24587,2458924592,24595	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych.
152.	13.09.2014 r. II SA/Wa 1360/14	DOLiS/DEC-518/14/42501,42508	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – odrzucenie skargi
153.	24.09.2014 r. II SA/Wa 1000/14	DOLiS/DEC-299/14/24587,2458924592,24595	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych.
154.	24.09.2014 r. II SA/Wa 2200/13	DOLiS/DEC-498/12/34135,34141	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - stwierdzenie nieważności zaskarżonej decyzji oraz poprzedzającej ją decyzji i określenie, że zaskarżona decyzja nie podlega wykonaniu.
155.	24.09.2014 r. II SAB/Wa 547/14	Dot. DOLiS-440-1525/12	Skarga na przewlekłe prowadzenie postępowania przez GIODO w przedmiocie ochrony danych osobowych	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych.
156.	30.09.2014 r. II SA/Wa 841/14	DOLiS/DEC-153/14/13124,13128,13132,13134	Skarga na decyzję w przedmiocie odmowy uwzględnienia skargi na przetwarzanie danych osobowych	Postanowienie WSA o przyznaniu prawa pomocy w zakresie obejmującym zwolnienie od kosztów sądowych oraz ustanowienie adwokata.
157.	01.10.2014 r. I OSK 601/13	DRZDO-DEC/499/12/34360	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 20.11.2012 r. II SA/Wa 1474/12 oddalającego skargę na decyzję w przedmiocie umorzenia postępowania w sprawie zgłoszenia zmian w zbiorze danych	Wyrok NSA – oddalenie skargi kasacyjnej
158.	01.10.2014 r. I OSK 873/13	DRZDO-DEC/500/12/34361	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 09.01.2013 r. II SA/Wa 1475/12 oddalającego skargę na decyzję	Wyrok NSA – oddalenie skargi kasacyjnej

			w przedmiocie umorzenia postępowania w sprawie zgłoszenia zmian w zbiorze danych	
159.	01.10.2014 r. I OSK 945/13	DRZDO-DEC/501/12/34362	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 09.01.2013 r. II SA/Wa 1476/12 oddalającego skargę na decyzję w przedmiocie umorzenia postępowania w sprawie zgłoszenia zmian w zbiorze danych	Wyrok NSA – oddalenie skargi kasacyjnej
160.	02.10.2014 r. II SAB/Wa 446/14	DOLiS-440-1262/13	Skarga na bezczynność organu w przedmiocie rozpoznania wniosku o udostępnienie danych osobowych	Postanowienie WSA – odrzucenie skargi
161.	08.10.2014 r. II SAB/Wa 63/14	DOLiS-440-270/13	Skarga na bezczynność organu w przedmiocie rozpoznania wniosku	Wyrok WSA stwierdzający, że bezczynność nie miała miejsca z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie.
162.	09.10.2014 r. II SAB/Wa 411/14	DOLiS-440-1188/13	Skarga na przewlekłość organu	Wyrok WSA stwierdzający, że przewlekłość organu miała miejsce z rażącym naruszeniem prawa, oraz wymierzający grzywnę w wysokości 2000 zł, a w pozostałym zakresie umarzający postępowanie.
163.	09.10.2014 r. II SA/Wa 2394/13	DOLiS/DEC-1186/13/75909,75916	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych.
164.	09.10.2014 r. II SAB/Wa 38/14	DOLiS-440-389/13	Skarga na bezczynność organu w przedmiocie rozpatrzenia skargi w sprawie nieprawidłowości w procesie przetwarzania danych osobowych	Wyrok WSA stwierdzający, że bezczynność organu miała miejsce z rażącym naruszeniem prawa, oraz wymierzający grzywnę w wysokości 2000 zł, a w pozostałym zakresie umarzający postępowanie.
165.	09.10.2014 r. II SA/Wa 790/14	DOLiS/DEC-142/14/12402,12408,12411	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia pełnomocnika.
166.	10.10.2014 r. II SAB/Wa 586/14	DOLiS-440-1126/12	Skarga na przewlekłość w prowadzeniu postępowania przez GIODO w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – przyznanie prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika.
167.	10.10.2014 r. II SA/Wa 1502/14	DOLiS/DEC-507/14/41187, 41198	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – przyznanie prawa pomocy w zakresie zwolnienia od kosztów sądowych i ustanowienia pełnomocnika.
168.	14.10.2014 r. II SA/Wa 1789/13	DOLiS/DEC-727/13/43820,43822-	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA odmawiające przyznanie pełnomocnikowi wynagrodzenia za zastępstwo prawne.
169.	16.10.2014 r.	DOLiS/DEC-	Skarga na decyzję w przedmiocie	Postanowienie WSA – odrzucenie

	II SA/Wa 1002/14	593/13/33418,334 23,33425,33429	ochrony danych osobowych	zażalenia na postanowienie WSA w Warszawie z dnia 12.12.2014 r., sygn. akt II SA/Wa 1002/14.
170.	17.10.2014 r. II SAB/Wa 879/14	DOLiS-440-1306/12	Skarga na przewlekłość postępowania w rozpatrzeniu skargi na nieprawidłowości w procesie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
171.	23.10.2014 r. II SAB/Wa 277/14	DOLiS-440-535/13	Skarga na przewlekłe prowadzenie postępowania w sprawie skargi na przetwarzanie danych osobowych	Postanowienie WSA – odrzucenie skargi
172.	24.10.2014 r. II SAB/Wa 615/14	DOLiS-440-1258/13	Skarga na bezczynność organu w przedmiocie rozpatrzenia skargi w sprawie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
173.	24.10.2014 r. II SA/Wa 717/14	DOLiS/DEC-170/14/14185,141 96	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
174.	24.10.2014 r. I OSK 1663/13	DOLiS/DEC-1170/12/71238, 71242	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 4.04.2013 r. sygn. akt II SA/Wa 189/13 w sprawie ze skargi na decyzję w przedmiocie odmowy uwzględnienia wniosku na odmowę udostępnienia danych osobowych użytkowników działek	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 4.04.2013 r. sygn. akt II SA/Wa 189/13.
175.	24.10.2014 r. II SA/Wa 1604/14	DOLiS/DEC-639/14/50917,509 22	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
176.	28.10.2014 r. II SA/Wa 166/14	DOLiS/DEC-1191/13/76231,76 243	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA uchylający zaskarżoną decyzję w części utrzymującej w mocy decyzję w zakresie pkt 2; oraz oddalający skargę w pozostałym zakresie.
177.	30.10.2014 r. II SAB/Wa 601/14	DOLiS-440-1708/13	Skarga na bezczynność organu w przedmiocie rozpatrzenia skargi w sprawie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
178.	04.11.2014 r. II SAB/Wa 616/14	DOLiS-440-1257/13	Skarga na bezczynność organu w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
179.	06.11.2014 r. II SA/Wa 458/14	DOLiS/DEC-863/13/54044,540 52	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
180.	06.11.2014 r. I OZ 981/14	DOLiS-440-1525/12	Skarga na przewlekłe prowadzenie postępowania przez GIODO w przedmiocie ochrony danych osobowych	Postanowienie NSA – oddalenie zażalenia na postanowienie WSA w Warszawie z dnia 24.09.2014 r., sygn. akt II SAB/Wa 547/14.
181.	07.11.2014 r. II SA/Wa 644/14	DOLiS/DEC-64/14/7471,7476	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
182.	12.11.2014 r. II SAB/Wa 32/14	DOLiS-440-931/12	Skarga na bezczynność organu w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający, że bezczynność organu nie miała miejsca z rażącym naruszeniem

				prawa, oraz umarzający postępowanie w pozostałym zakresie.
183.	13.11.2014 r. II SAB/Wa 644/14	DOLiS-440-1122/12	Skarga na bezczynność organu w przedmiocie rozpoznania wniosku o ponowne rozpatrzenie sprawy	Postanowienie WSA - przyznanie prawa pomocy w zakresie zwolnienia od kosztów sądowych.
184.	13.11.2014 r. II SAB/Wa 288/14	DOLiS-440-1027/12	Skarga na bezczynność organu w przedmiocie wydania decyzji po złożeniu wniosku o ponowne rozpatrzenie sprawy	Wyrok WSA stwierdzający, że bezczynność organu miała miejsce z rażącym naruszeniem prawa, oraz wymierzający GIODO grzywnę w wysokości 1000 zł., zaś w pozostałym zakresie umarzający postępowanie.
185.	13.11.2014 r. II SA/Wa 875/14	DOLiS/DEC-264/14/21131,21146	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku	Wyrok WSA - uchylenie zaskarżonej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
186.	19.11.2014 r. II SA/Wa 727/14	DOLiS/DEC-171/14/14199,14202	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
187.	19.11.2014 r. II SAB/Wa 391/14	DOLiS-440-167/14	Skarga na przewlekłe prowadzenie postępowania przez organ w przedmiocie ochrony danych osobowych	Wyrok WSA - zobowiązanie GIODO do rozpatrzenia wniosku skarżącego w terminie 30 dni od daty doręczenia prawomocnego wyroku oraz stwierdzenie, że przewlekłe prowadzenie postępowania przez organ miało miejsce z rażącym naruszeniem prawa.
188.	20.11.2014 r. I OSK 2846/14	DOLiS/DEC-25/14/4154,4156	Skarga na decyzję w przedmiocie przetwarzania osobowych	Postanowienie NSA – wstrzymanie wykonania zaskarżonej decyzji.
189.	20.11.2014 r. II SAB/Wa 437/14	DOLiS-440-21/12	Skarga na bezczynność organu w przedmiocie przetwarzania danych osobowych	Wyrok WSA stwierdzający, że bezczynność nie miała miejsca z rażącym naruszeniem prawa, zaś w pozostałym zakresie umarzający postępowanie.
190.	25.11.2014 r. II SA/Wa 376/14	DOLiS/POST-6/14/882	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Postanowienie WSA - zasądzenie kosztów nieopłaconej pomocy prawnej udzielonej z urzędu.
191.	26.11.2014 r. II SA/Wa 456/14	DOLiS/DEC-1350/13/86490,86508	Skarga na decyzję w przedmiocie przetwarzania osobowych	Wyrok WSA – oddalenie skargi
192.	26.11.2014 r. II SA/Wa 1222/14	DOLiS/DEC-828/13/49462,49465	Skarga na decyzję w przedmiocie przetwarzania osobowych	Wyrok WSA - uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji oraz określenie, że zaskarżona decyzja nie podlega wykonaniu w całości.
193.	27.11.2014 r. II SA/Wa 792/14	DOLiS/DEC-173/14/14255,14257,14259	Skarga na decyzję w przedmiocie przetwarzania osobowych	Wyrok WSA – oddalenie skargi
194.	12.12.2014 r. II SA/Wa 475/14	DOLiS/DEC-38/14/5458,5463	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie przetwarzania danych osobowych i niespełnienia	Wyrok WSA – oddalenie skargi

			obowiązku informacyjnego	
195.	17.12.2014 r. II SA/Wa 132/12	DOLiS/POST-101/09/14892, 14893	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku	Postanowienie WSA - przyznanie kosztów nieopłaconej pomocy prawnej udzielonej z urzędu.
196.	18.12.2014 r. II SAB/Wa 587/14	DOLiS-440-1358/13	Skarga na przewlekłe prowadzenie postępowania przez organ w przedmiocie udostępnienia danych osobowych	Wyrok WSA stwierdzający, że przewlekłe prowadzenie postępowania przez GIODO miało miejsce z rażącym naruszeniem prawa, oraz wymierzający grzywnę w wysokości 1000 zł., zaś w pozostałym zakresie umarzający postępowanie.
197.	18.12.2014 r. I OSK 900/13	DOLiS/DEC-1310/10/47273,47275	Skarga kasacyjna GIODO od wyroku WSA z dn. 07.06.2011 r. w sprawie ze skargi na decyzję w przedmiocie nakazu usunięcia uchybień powstałych w procesie przetwarzania danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 7.06.2011 r. sygn. akt II SA/Wa 267/11 i oddalający skargę.
198.	18.12.2014 r. II SA/Wa 1677/14	DOLiS/DEC-1008/11/57325,57327,57332	Skarga na decyzję w przedmiocie przetwarzania osobowych	Wyrok WSA – oddalenie skargi

Załącznik nr 4

Informacje przekazane przez organy ścigania w sprawach zawiadomień o popełnieniu przestępstwa skierowanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2014 r.

Informacja	**Rok 2012**	**Rok 2013**	**Rok 2014**
Umorzenie dochodzenia	9	5	1
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	-	-	-
Umorzenie dochodzenia i odmowa podjęcia go na nowo	-	-	-
Wszczęcie dochodzenia	-	2	3
Odmowa wszczęcia dochodzenia	3	3	2
Wszczęcie śledztwa i jego umorzenie	-	2	-
Zawieszenie dochodzenia	-	-	-
Skierowanie sprawy do sądu	-	-	-
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	1	-	-
Brak informacji	1	4	4

Załącznik nr 5

Wykaz szkoleń przeprowadzonych przez GIODO w 2014 r.

L.p.	Data szkolenia	Podmiot szkolony	Miejscowość
1.	15.01.2014	Ministerstwo Sportu i Turystyki	Warszawa
2.	15.01.2014	Komenda Główna Policji	Warszawa
3.	15.01.2014	Urząd Miasta st. Warszawy	Warszawa
4.	16.01.2014	Urząd Miasta st. Warszawy	Warszawa
5.	30.01.2014	Lekcja nt. ochrony danych osobowych dla uczniów gimnazjum	Warszawa
6.	19.02.2014	Urząd Miasta st. Warszawy	Warszawa
7.	20.02.2014	Urząd Miasta st. Warszawy	Warszawa
8.	11.03.2014	Laboratorium Kryminalistyczne Komendy Stołecznej Policji	Warszawa
9.	18.03.2014	Laboratorium Kryminalistyczne Komendy Stołecznej Policji	Warszawa
10.	20.03.2014	Urząd Miasta st. Warszawy	Warszawa
11.	24.03.2014	Ministerstwo Spraw Zagranicznych	Warszawa
12.	26.03.2014	Szkolenie on-line dla szkół i ośrodków doskonalenia zawodowego nauczycieli w ramach Programu GIODO „Twoje dane – twoja sprawa. (...)"	Warszawa
13.	26.03.2014	Okręgowa Izba Radców Prawnych	Opole
14.	28.03.2014	Urząd Miasta Rzeszowa	Rzeszów
15.	31.03.2014	Urząd Miasta Rzeszowa	Rzeszów
16.	03.04.2014	Okręgowa Izba Radców Prawnych	Katowice
17.	08.04.2014	Centrum Operacji Specjalnych – Dowództwo Komponentów Wojsk Specjalnych	Warszawa
18.	18.04.2014	Urząd Marszałkowski Województwa Śląskiego	Katowice
19.	24.04.2014	Okręgowa Izba Radców Prawnych	Legnica
20.	25.04.2014	Okręgowa Izba Radców Prawnych	Zielona Góra
21.	26.04.2014	Okręgowa Izba Radców Prawnych	Gorzów Wlkp.
22.	05.05.2014	Okręgowa Izba Radców Prawnych	Lublin
23.	06.05.2014	Okręgowa Izba Radców Prawnych	Warszawa
24.	12.05.2014	Okręgowa Izba Radców Prawnych	Łódź
25.	15.05.2014	Okręgowa Izba Radców Prawnych	Szczecin
26.	16.05.2014	Okręgowa Izba Radców Prawnych	Koszalin
27.	21.05.2014	Szkoła Policji w Katowicach	Katowice
28.	26.05.2014	Okręgowa Izba Radców Prawnych	Kalisz
29.	27.05.2014	Okręgowa Izba Radców Prawnych	Poznań

30.	29.05.2014	Okręgowa Izba Radców Prawnych	Kielce
31.	03.06.2014	Państwowa Inspekcja Pracy	Wrocław
32.	04.06.2014	Okręgowa Izba Radców Prawnych	Rzeszów
33.	14.06.2014	Okręgowa Izba Radców Prawnych	Kraków
34.	17.06.2014	Okręgowa Izba Radców Prawnych	Białystok
35.	23.06.2014	Urząd Miasta Gdyni	Gdynia
36.	24.06.2014	Urząd Miasta w Gdańsku	Gdańsk
37.	24.06.2014	Regionalna Izba Gospodarcza Pomorza, Związek Pracodawców Pomorza, Gdański Park Naukowo-Techniczny	Gdańsk
38.	25.06.2014	Urząd Miejski w Wejherowie	Wejherowo
39.	25.06.2014	Sąd Okręgowy w Gdańsku	Gdańsk
40.	26.06.2014	Okręgowa Izba Radców Prawnych	Toruń
41.	27.06.2014	Okręgowa Izba Radców Prawnych	Bydgoszcz
42.	03.07.2014	Rządowe Centrum Legislacji	Warszawa
43.	11.07.2014	Okręgowa Izba Radców Prawnych	Olsztyn
44.	26.08.2014	Komenda Główna Policji	Polańczyk
45.	04.09.2014	Ministerstwo Spraw Zagranicznych	Warszawa
46.	12.09.2014	Krajowa Rada Doradców Podatkowych	Białobrzegi
47.	13.09.2014	Krajowa Rada Radców Prawnych	Kraków
48.	22.09.2014	Kancelaria Senatu	Warszawa
49.	06.10.2014	Ministerstwo Sprawiedliwości	Warszawa
50.	8.10.2014	Prokuratura Okręgowa – szkolenie dla prokuratorów	Warszawa
51.	15.10.2014	Prokuratura Okręgowa – szkolenie dla urzędników	Warszawa
52.	17.10.2014	Centralne Biuro Antykorupcyjne	Warszawa
53.	22.10.2014	Starogardzki Klub Biznesu	Starogard Gdański
54.	23-24.10.2014	Szkolenie w ramach programu „Twoje dane – twoja sprawa (...)"	Warszawa
55.	27.10.2014	Krajowa Izba Doradców Podatkowych	Warszawa
56.	28-29.10.2014	Komenda Wojewódzka Policji w Olsztynie	Olsztyn
57.	14.11.2014	Ministerstwo Gospodarki	Huta Żabiowolska
58.	13.11.2014	Ministerstwo Spraw Zagranicznych	Warszawa
59.	19.11.2014	Warszawska Opera Kameralna	Warszawa
60.	21.11.2014	Urząd Ochrony Konkurencji i Konsumentów	Warszawa
61.	25.11.2014	Ministerstwo Spraw Wewnętrznych	Warszawa
62.	26-27.11.2014	Ministerstwo Administracji i Cyfryzacji	Popowo
63.	11.12.2014	Warszawski Uniwersytet Medyczny	Warszawa
64.	11.12.2014	Urząd Miasta Krakowa	Kraków

Załącznik nr 6

Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych w 2014 r.

1. Światowy Dzień Społeczeństwa Informacyjnego (ŚDSI) w Polsce w 2014 r. Organizator: Polskie Towarzystwo Informatyczne.
2. III Świętokrzyski Dzień Bezpiecznego Internetu – 28 stycznia 2014 r. Organizator: Wyższa Szkoła Ekonomii, Prawa i Nauk Medycznych im. Profesora Edwarda Lipińskiego w Kielcach.
3. III Małopolski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Inwałd k/Wadowic, 6-7 lutego 2014 r.
4. III Łódzki Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Smardzewice, 13-14 lutego 2014 r.
5. Konferencja „Bezpieczeństwo w cyberprzestrzeni – czyli jak chronić tożsamość w Internecie". Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland. Warszawa, 5 marca 2014 r.
6. XIII edycja Konferencji z cyklu „Social Media Day Poland'. Organizator: Publicon Sp. z o.o. Wrocław, 6 marca 2014 r.
7. XIV Sympozjum Świata Telekomunikacji i Mediów oraz XVI Wielka Gala Złotych Anten Świata Telekomunikacji i V Wielka Gala Kryształowych Anten Świata Mediów. Organizator: MM Conferences. Warszawa, 12-13 marca 2014 r.
8. Konferencja „IT w Służbie Zdrowia". Organizator: IDG Poland, Magazyn Menedżerów i Informatyków Computerworld. Warszawa, 20 marca 2014 r.
9. IV Konferencja Naukowa „Ataki Sieciowe 2014". Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii działające na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu oraz Centrum Badań nad Cyberprzestępczością. Toruń, 24 marca 2014 r.
10. Konferencja „Dyrektor XXI wieku – mobilność, bezpieczeństwo, innowacyjność". Organizator: firma Librus. Ożarów Mazowiecki, 24-25 marca 2014 r.
11. VII Konferencja SEMAFOR (Security, Management, Audit, Forum). Organizator: magazyn Computerworld oraz stowarzyszenia ISSA Polska i ISACA Warsaw Chapter. Warszawa, 27-28 marca 2014 r.
12. Konkurs wiedzy dla uczniów częstochowskich szkół. Organizator: Zespół Szkół Samochodowo-Budowlanych, kwiecień 2014 r.
13. Forum IT dla Kierowników w Administracji. Organizator: Redakcja „IT w Administracji". Zakopane, 3-4 kwietnia 2014 r.
14. Międzynarodowe Targi Zabezpieczeń SECUREX 2014, organizowane w ramach Międzynarodowych Targów Poznańskich. Poznań, 8-11 kwietnia 2014 r.

15. IV Dolnośląski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Świeradów Zdrój, 10-11 kwietnia 2014 r.
16. III Otwarty Kongres FLOSS. Organizator: Instytut Informatyki i Nauki o Materiałach Uniwersytetu Śląskiego w Katowicach oraz Polska Grupa Użytkowników Linuxa (PLUG). Sosnowiec, 12 kwietnia 2014 r.
17. Symulacja obrad Parlamentu Europejskiego i Rady (Model European Union – MEU). Organizator: Stowarzyszenie BETA Polska. Warszawa, 9-14 maja 2014 r.
18. Ogólnopolska Konferencja Naukowa pt. „Nowe regulacje rynku usług płatniczych i pieniądza elektronicznego". Organizator: Centrum Prawa Nowych Technologii Wydziału Prawa i Administracji UW. Warszawa, 13 maja 2014 r.
19. X Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Zakopane, 28-30 maja 2014 r.
20. IV Mazowiecki Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Rawa Mazowiecka, 29-30 maja 2014 r.
21. Konferencja pt. „Ochrona danych osobowych w działalności kościołów i związków wyznaniowych". Organizator: Centrum Ochrony Danych Osobowych Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 30 maja 2014 r.
22. II Wiosenny Konwent Ochrony Danych i Informacji. Organizator: FORSAFE Sp. z o.o. Łódź, 15 maja 2014 r.
23. 3. Międzynarodowa Konferencja Ciągłości Działania pt. „Zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów Państwa w obliczu dzisiejszych zagrożeń". Organizator: Wyższa Szkoła Policji w Szczytnie oraz British Standards Institution Group Polska. Szczytno, 3-4 czerwca 2014 r.
24. VIII Konferencja FORUM IAB Polska. Organizator: Związek Pracodawców Branży Internetowej IAB Polska. Warszawa, 4-5 czerwca 2014 r.
25. VI Konferencja „International Biometric Congress". Organizator: Związek Banków Polskich. Miedzeszyn, 5-6 czerwca 2014 r.
26. III Warmińsko-Mazurski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Mrągowo, 5-6 czerwca 2014 r.
27. II Polski Kongres Prawa Własności Intelektualnej 2014. Organizator: Instytut Allerhanda. Warszawa, 10 czerwca 2014 r.
28. IV Śląski Konwent Informatyków i Administracji. Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Hotel Zawiercie Business & Leisure, Zawiercie, 12-13 czerwca 2014 r.
29. Konferencja „Pięć żywiołów. Wolność – informacja – bezpieczeństwo". Organizatorzy: Fundacja „Instytut Mikromakro", Ośrodek Badań nad Przyszłością Collegium Civitas, Stowarzyszenie Euro-Atlantyckie oraz Przemysłowy Instytut Automatyki i Pomiarów – PIAP. Warszawa, 16-18 czerwca 2014 r.
30. 13. Bałtyckie Targi Militarne BALT-MILITARY-EXPO. Organizator: Międzynarodowe Targi Gdańskie S.A. Gdańsk, 24-26 czerwiec 2014 r.

31. VII Konwent Informatyków i Administracji Pomorza i Kujaw. Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Ciechocinek, 26-27 czerwca 2014 r.
32. I Śląski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji", Ustronie, 10-11 lipca 2014 r.
33. Debata internetowa „Jak chronić swoją prywatność w Internecie?". Organizatorzy: Onet.pl oraz PCLab.pl. Warszawa, 15 lipca 2014 r.
34. III Lubelski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Janów Lubelski, 28-29 sierpnia 2014 r.
35. Wystawa pt. „Dokumenty tożsamości". Organizator: Muzeum Warmii i Mazur. Morąg, sierpień 2014 r.
36. Biometric Summit – oblicza uwierzytelniania tożsamości". Organizator: MultiTrain. Warszawa, 4 września 2014 r.
37. IV Lubuski Konwent Informatyków i Administracji. Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Jesionka, 4-5 września 2014 r.
38. Konferencja ESORICS'2014 – 9. European Symposium on Research in Computer Security. Organizator: Politechnika Wrocławska. Wrocław, 7-9 września 2014 r.
39. III Pomorski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Jastrzębia Góra, 11-12 września 2014 r.
40. VII Forum Dyrektorów Działów Prawnych. Organizator: Puls Biznesu. Warszawa, 17-18 września 2014 r.
41. VII Zachodniopomorski Konwent Informatyków i Administracji. Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Dwór Pomorski Luboradza, 18-19 września 2014 r.
42. 3. Międzynarodowa Konferencja Ciągłości Działania pt. „Zapewnienie bezpieczeństwa i ciągłości funkcjonowania organów Państwa w obliczu dzisiejszych zagrożeń". Organizator: Wyższa Szkoła Policji w Szczytnie oraz British Standards Institution Group Polska. Szczytno, 23-24 września 2014 r.
43. VII 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, 24 – 25 września 2014 r.
44. III Wielkopolski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Trzebaw k/Poznania, 25-26 września 2014 r.
45. Podkarpacki Konwent Informatyków i Administracji. Organizator: Oddział Regionalny Szczecińskiego Parku Naukowo-Technologicznego z siedzibą w Bydgoszczy. Nowy Dwór, 2-3 października 2014 r.
46. III Podkarpacki Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Polańczyk nad Soliną, 23-24 października 2014 r.
47. Think Big Congress: BIG DATA. Organizator: MM Conferences S.A. Warszawa, 5-6 listopada 2014 r.

48. XIII Konferencja „Systemy Informatyczne w Energetyce". Organizator: Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej. Wisła, 25-28 listopada 2014 r.
49. Konferencja „Security Case Study 2014". Organizator: Fundacja Bezpieczna Cyberprzestrzeń. Warszawa, 26-27 listopada 2014 r.
50. V Krajowe Forum Kierowników Jednostek Organizacyjnych oraz IX Forum Pełnomocników ds. Ochrony Informacji Niejawnych. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Szczyrk, 3-5 grudnia 2014 r.
51. I Kujawsko-Pomorski Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Brzoza k/Bydgoszczy, 4-5 grudnia 2014 r.

Załącznik nr 7

Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2014 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty

l.p.	Data	Konferencja/Seminarium	Miejsce
1.	23.01.2014	Konferencja „Przeszłość, teraźniejszość i przyszłość ochrony informacji niejawnych w zapewnianiu bezpieczeństwa narodowego RP". Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.	Pułtusk
2.	28.01.2014	VIII Dzień Ochrony Danych Osobowych. Konferencja „Prywatność w cyfrowym świecie". Organizator: GIODO.	Warszawa
3.	30.01.2014	Spotkanie Generalnego Inspektora Ochrony Danych Osobowych z uczniami Gimnazjum Nr 132 z Oddziałami Integracyjnymi w Warszawie.	Warszawa
4.	18.02.2014	Spotkanie eksperckie poświęcone kwestii zgodności przepisów prawa polskiego z przepisami Konwencji o ochronie praw człowieka i godności istoty ludzkiej w odniesieniu do biologii i medycyny. Organizator: Pełnomocnik Rządu ds. Równego Traktowania, Kancelaria Prezesa Rady Ministrów.	Warszawa
5.	26.02.2014	Konferencja „ Gruźlica powraca – prawda czy mit". Organizatorzy: Małopolskie Kuratorium Oświaty, Kuratorium Oświaty w Krakowie oraz Wojewódzki Szpital Chorób Płuc i Rehabilitacji.	Kraków
6.	19-21.03.2014	II Konferencja „Safety and Security – Nowoczesne technologie, systemy i rozwiązania organizacyjne dla bezpieczeństwa informacji i danych osobowych". Organizatorzy: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego.	Pułtusk
7.	24.03.2014	IV Ogólnopolska Konferencja Naukowa „Ataki Sieciowe 2014". Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii Wydziału Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu oraz Centrum Badań nad Cyberprzestępczością.	Toruń
8.	26.03.2014	Debata pt. „Ochrona danych osobowych a wybory" . Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją Wydziału Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
9.	27-28.03.2014	VII Konferencja SEMAFOR (Security, Management, Audit, Forum). Organizatorzy: magazyn Computerworld oraz stowarzyszenia ISSA Polska i ISACA Warsaw Chapter.	Warszawa
10.	31.03.2014	Konferencja „E-protokół a wymiar sprawiedliwości". Organizator: Stowarzyszenie Sędziów Polskich IUSTITIA.	Warszawa
11.	3-4.04.2014	Forum IT dla Kierowników w Administracji Publicznej. Organizator: miesięcznik „IT w Administracji".	Zakopane
12.	8-11.04.2014	20. edycja Międzynarodowych Targów Zabezpieczeń SECUREX. Organizator: Międzynarodowe Targi Poznańskie.	Poznań
13.	9-10.04.2014	Konferencja „Energetyka +". Organizator: Trio Conferences.	Warszawa
14.	10.04.2014	Debata pt.: Ochrona danych osobowych a wykonywanie zawodów prawniczych. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją Wydziału Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
15.	13.05.2014	Ogólnopolska Konferencja Naukowa „Nowe regulacje rynku	Warszawa

		usług płatniczych i pieniądza elektronicznego. Organizatorzy: Centrum Prawa Nowych technologii Wydziału prawa i Administracji Uniwersytetu Warszawskiego we współpracy z Instytutem Zmian.	
16.	15.05.2014	II Wiosenny Konwent Ochrony Danych i Informacji. Organizator: Forsafe Sp. z o. o.	Łódź
17.	20-21.05.2014	VI Forum Technologii Bankowości Spółdzielczej 2014. Organizator: Centrum Prawa Bankowego i Informacji, Związek Banków Polskich.	Warszawa
18.	23.05.2014	Konferencja Naukowa pt. „Jawność i tajność a sprawność administrowania" w ramach projektu badawczo-rozwojowego „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", realizowanego na rzecz bezpieczeństwa i obronności państwa.	Warszawa
19.	27.05.2014	Konferencja „Czego możemy oczekiwać po wirtualnych urzędach? Szanse i zagrożenia dla rozwoju e-administracji w Polsce". Organizator: Koło Naukowe Administracji Publicznej (KNAP) działające na Wydziale Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego.	Warszawa
20.	30.05.2014	Konferencja „Ochrona danych osobowych w działalności Kościołów i innych związków wyznaniowych". Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją Wydziału Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
21.	24.06.2014	Spotkanie z delegacją tokijskiego instytutu IISE (Institute for International Socio-Economic Studies), podczas odbywających się w Trójmieście IV Dni Otwartych GIODO.	Gdańsk
22.	25.06.2014	Warsztaty podsumowujące projekt partnerski LdV „Raising awareness of the data protection issues among the employees working in the EU".	Gdańsk
23.	7-10.07.2014	Wizyta delegacji Krajowej Agencji Ochrony Danych Osobowych Kosowa w Biurze GIODO.	Warszawa
24.	28-29.07.2014	Inauguracyjne spotkanie Zespołu Zadaniowego ds. ochrony cyberprzestrzeni RP.	Warszawa
25.	17.09.2014	Seminarium nt. wykorzystania biometrii i innych nowoczesnych technologii w ochronie infrastruktury krytycznej. Organizator: Rządowe Centrum Bezpieczeństwa.	Warszawa
26.	23-24.09.2014	Wizyta delegacji słowackiego Urzędu Ochrony Danych Osobowych w Biurze GIODO.	Warszawa
27.	24.09.2014	III Konferencja Zarządzania Ciągłością Działania pt. „Zapewnienie Bezpieczeństwa i Ciągłości Funkcjonowania Organów Państwa w Obliczu Dzisiejszych Zagrożeń". Organizatorzy: Wyższa Szkoła Policji w Szczytnie oraz British Standard Institution (BSI).	Szczytno
28.	8-10.10.2014	IV Konferencja Bezpieczeństwa Narodowego. Organizatorzy: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego.	Spała
29.	20.10.2014	Konferencja Naukowa pt. „Perspektywy zmian regulacji jawności i jej ograniczeń" w ramach projektu badawczo-rozwojowego „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", realizowanego na rzecz bezpieczeństwa i obronności państwa.	Warszawa
30.	21-22.10.2014	Konferencja Naukowa pt. „Jawność i ograniczenia jawności publicznych zasobów informacyjnych" w ramach projektu badawczo-rozwojowego „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", realizowanego na rzecz bezpieczeństwa i obronności państwa.	Kazimierz Dolny
31.	29.10.2014	Konferencja „Lawyers in the Media Society". Organizator:	Łódź

		Wydział Prawa i Administracji Uniwersytetu Łódzkiego.	
32.	14.11.2014	9. doroczna Konferencja Zakładu Praw Człowieka Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, pt. „Wpływ Europejskiej Konwencji Praw Człowieka na funkcjonowanie biznesu".	Warszawa
33.	17.11.2014	Seminarium pt. „Sędzia – osoba publiczna czy prywatna? Granice dostępu do informacji publicznej i ochrony danych osobowych". Organizatorzy: Sąd Apelacyjny w Łodzi, Oddział Łódzki Stowarzyszenia Sędziów Polskich IUSTITIA, Centrum ochrony Danych Osobowych i Zarządzania Informacją Wydziału Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
34.	21.11.2014	Spotkanie GIODO z przedsiębiorcami. Organizator: Iron Mountain.	Kraków
35.	24.11.2014	Konferencja Naukowa „Prywatność i jawność: bilans 25-lecia". Organizatorzy: GIODO, Dziekan Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, Koło Naukowe „CyberLaw", Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW.	Warszawa
36.	25.11.2014	IV edycja Central Eastern Europe Fraud and Risk Conference „Risk & Security Management. From Know-How to How Do".	Warszawa
37.	3.12.2014	Debata pt. „Prawo do informacji a prawo do prywatności". Organizatorzy: GIODO oraz Dziennik Gazeta prawna.	Warszawa
38.	10.12.2014	Konferencja Naukowa pt. „Retencja danych telekomunikacyjnych – praktyka, orzecznictwo, postulaty *de lege ferenda*". Organizatorzy: Naczelna Rada Adwokacka i Krajowa Izba Radców Prawnych.	Warszawa
39.	12.12.2014	Konferencja „Egzekwowanie prywatności: wnioski z obecnego wdrażania i perspektywy na przyszłość", kończąca projekt PHAEDRA, realizowany przez GIODO, Vrije Universiteit Brussel (VUB-LSTS) z Belgii, Trilateral Research & Consulting LLP z Wielkiej Brytanii oraz Universitat Jaume I z Hiszpanii.	Kraków
40.	15.12.2014	VII Forum Nowej Gospodarki pt. „Kierunek – Miasto Przyszłości". Organizator: Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie.	Kraków

Załącznik nr 8

Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2014 r. za granicą

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	14.01.2014	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
2.	15-16.01.2014	Spotkanie Podgrupy ds. Technologii.	Bruksela
3.	20.01.2014	Konferencja z okazji 10-lecia urzędu Europejskiego Inspektora Ochrony Danych.	Bruksela
4.	21.01.2014	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
5.	22.01.2014	Międzynarodowa Konferencja z okazji obchodów VIII Europejskiego Dnia Ochrony Danych Osobowych pt. The Computers, Privacy and Data Protection Conference – CPDP 2014. Reforming Data Protection: the Global Perspective.	Bruksela
6.	24.01.2014	Spotkanie partnerów projektu PHAEDRA z przedstawicielami europejskich organów ochrony danych osobowych oraz rzeczników prywatności i innych instytucji zajmujących się ochroną prywatności na poziomie ogólnoświatowym.	Bruksela
7.	3-5.02.2014	Assert Master Class, University of Stirling.	Edynburg
8.	19-22.02.2014	Spotkanie w ramach projektu partnerskiego Leonardo da Vinci (LdV).	Zagrzeb
9.	26-27.02.2014	94. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
10.	28.02.2014	Spotkanie europejskich organów ochrony danych w sprawie zastosowań zdalnie sterowanych systemów lotniczych (RPAS).	Bruksela
11.	28.02.2014	High Level Conference on the EU Cybersecurity Strategy. Organizator: Komisja Europejska we współpracy z Europejską Służbą Działań Zewnętrznych.	Bruksela
12.	11.03.2014	Second meeting on notification of personal data breaches under the ePrivacy Directive and the Commission Regulation.	Bruksela
13.	18-20.03.2014	Posiedzenie Wspólnego Organu Nadzorczego Europolu oraz Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
14.	20.03.2014	Meeting of the European Multi-Stakeholder Forum on Electronic invoicing.	Bruksela
15.	20-21.03.2014	Warsztaty nt. zagrożeń ochrony prywatności oraz obrady Okrągłego Stołu ekspertów OECD nt. Big Data oraz analityki (Privacy Risk Framework Project Workshop I).	Paryż
16.	24.03.2014	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela
17.	1-4.04.2014	16. Spotkanie Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA).	Skopje
18.	1-4.04.2014	International Enforcement Coordination Annual Event - doroczna konferencja poświęcona międzynarodowemu egzekwowaniu prawa. Organizator: Information Commissioner's Office - ICO	Manchester
19.	7-9.04.2014	Brussels Forum (Forum do spraw prawno-ekonomicznych pomiędzy Unią Europejską a Stanami Zjednoczonymi).	Bruksela
20.	8.04.2014	Warsztaty nt. certyfikatów ochrony prywatności UE.	Bruksela
21.	8-9.04.2014	95. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela

22.	9.04.2014	Konferencja pt. „Zbiory danych, informowanie obywateli: paszport do ochrony danych osobowych". Organizator: Europejskie Stowarzyszenie Ochrony Praw Człowieka (AEDH), francuska Liga Praw Człowieka (LDH), węgierskie stowarzyszenie Unia Praw Obywatelskich, niemieckie stowarzyszenie Humanistische Union, luksemburska Liga Praw Człowieka (ALOS-LDH) oraz Europejskie Stowarzyszenie Sędziów i Prokuratorów na rzecz Demokracji i Wolności (MEDEL - European Magistrates for Democracy and Freedom).	Bruksela
23.	29.04.-2.05.2014	Międzynarodowa Konferencja „Data Protection Intensive". Organizator: The International Association of Privacy Professionals.	Londyn
24.	4-7.05.2014	2. Warsztaty projektu PHAEDRA pn. „Wyzwania i bariery współpracy i koordynacji działań pomiędzy organami ochrony danych osobowych (DPAs).	Skopje
3.	5-6.05.2014	55. posiedzenie Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupy Berlińskiej).	Skopje
4.	6-8.05.2014	Posiedzenie Grypy Koordynującej Nadzór nad VIS, SIS II, IMI i Eurodac.	Bruksela
5.	7-9.05.2014	Wizyta w Urzędzie Inspektora Ochrony Danych Osobowych Gruzji.	Tbilisi
6.	12-16.05.2014	Misja Ewaluacyjna - wdrożenie dorobku prawnego w zakresie dotyczącym ochrony danych osobowych przetwarzanych w systemie Schengen.	Berne
7.	13-14.05.2014	Spotkanie Podgrupy ds. Technologii.	Bruksela
8.	14-15.05.2014	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29 .	Bruksela
9.	19-22.05.2014	Cambridge Forum on International Privacy Law w Kildare Country.	Dublin
10.	21-23.05.2014	6th Global Information Accountability Dialogue. Organizatorzy: The Information Accountability Foundation and Information Commissioner's Office – ICO.	Londyn
11.	2-4.06.2014	31. Posiedzenie Plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD).	Strasburg
12.	3-4.06.2014	96. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
13.	5.06.2014	Konferencja Europejskich Organów Ochrony Danych pt. „Współpraca europejska i międzynarodowa w obszarze ochrony danych". Organizatorzy: Rada Europy oraz francuski organ ochrony danych – CNIL.	Strasburg
14.	12-13.06.2014	Data Breach Workshop	Ispra
15.	15-19.06.2014	41st Asia Pacific Privacy Authorities Forum – APPA oraz 3. Warsztaty projektu PHAEDRA pn. „Rozporządzenie UE o ochronie danych w perspektywie udoskonalenia współpracy na poziomie regionalnym pomiędzy organami ochrony danych osobowych (DPAs), rzecznikami ds. ochrony prywatności (PCs) oraz organami ds. egzekwowania ochrony danych osobowych i prywatności (PEAs)".	Seul
16.	16-17.06.2014	Posiedzenie Wspólnego Organu Nadzorczego Europolu.	Bruksela
17.	8-9.07.2014	Spotkanie Podgrupy ds. Technologii.	Bruksela
18.	15.07.2014	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) GR Art. 29.	Bruksela
19.	24.07.2014	Spotkanie GR Art. 29 z operatorami wyszukiwarek.	Bruksela
20.	26.08.2014	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
21.	10-12.09.2014	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela

22.	10-12.09.2014	Spotkanie z przedstawicielami Parlamentu Europejskiego i Komisji Europejskiej.	Bruksela
23.	15-19.09.2014	Czynności kontrolne Systemu Informatycznego Schengen (SIS II) w Wydziale Konsularnym Ambasady RP w Kopenhadze.	Kopenhaga
24.	15-19.09.2014	Czynności kontrolne Systemu Informatycznego Schengen (SIS II) w Wydziale Konsularnym Ambasady RP w Oslo.	Oslo
25.	16-17.09.2014	97. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
26.	23-24.09.2014	Posiedzenie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE).	Bruksela
27.	1.10.2014	Spotkanie w Parlamencie Europejskim.	Bruksela
28.	1-2.10.2014	Posiedzenie Wspólnego Organu Nadzorczego Europolu.	Bruksela
29.	5-7.10.2014	Warsztaty rozpatrywania spraw. Organizator: Macedoński Organ Ochrony Danych Osobowych.	Skopje
30.	7-8.10.2014	Posiedzenie COREPER.	Bruksela
31.	13-15.10.2014	56. posiedzenie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska).	Berlin
32.	13-16.10.2014	36. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności oraz 4. Warsztaty zorganizowane w ramach projektu PHAEDRA.	Port Louis, Mauritius
33.	15-17.10.2014	Spotkanie ekspertów SURPRISE. Organizator: European University Institute.	Florencja
34.	19-24.10.2014	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) w Wydziale Konsularnym Ambasady RP w Belgradzie.	Belgrad
35.	29-31.10.2014	Konferencja „Zabezpieczenie prawa do ochrony danych w Unii Europejskiej". Organizator: ERA – Academy of European Law.	Paryż
36.	6-7.11.2014	Spotkanie w ramach projektu ARCADES.	Bruksela
37.	6-8.11.2014	Warsztaty „Ochrona danych w postępowaniu przygotowawczym i zapobieganie oszustwom korporacyjnym".	Praga
38.	15-20.11.2014	International Association of Privacy Professionals (IAPP): Europejski Kongres Ochrony Danych.	Bruksela
39.	18-20.11.2014	ECTA Regulatory Conference 2014. Organizator: Europejskie Stowarzyszenie na rzecz Konkurencji w Telekomunikacji.	Bruksela
40.	20-21.10.2014	Posiedzenie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE).	Bruksela
41.	24-26.11.2014	98. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
42.	24-29.11.2014	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) w Wydziale Konsularnym Ambasady RP w Rzymie.	Rzym
43.	1-2.12.2014	Spotkanie koordynatorów projektu ARCADES.	Bruksela
44.	9-10.12.2014	Posiedzenie Wspólnego Organu Nadzorczego Europolu.	Bruksela