SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Generalny Inspektor Ochrony Danych Osobowych

Druk nr 582

Warszawa, 2 czerwca 2016 r.

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

pragnę złożyć na ręce Pana Marszałka

- Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2015.

Sprawozdanie stanowi wykonanie art.. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 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 wyrazami szacunku

(-) dr Edyta Bielak-Jomaa

Generalny Inspektor
Ochrony Danych Osobowych

SPRAWOZDANIE
Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W ROKU 2015

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r. poz. 2135 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 2015 r. do 31 grudnia 2015 r.

SPIS TREŚCI

Spis treści

Wprowadzenie 5

Część I. Źródła prawa w zakresie ochrony danych osobowych 5

1. Informacje ogólne 5
2. Reforma prawa Unii Europejskiej w zakresie ochrony danych osobowych 11
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 2015 r. 16

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 18
2.1. Czynności kontrolne 18
2.2. Kontrola przetwarzania danych osobowych w wybranych obszarach 20
2.3. Systemy informatyczne służące do przetwarzania danych osobowych. 66
2.4. Wyniki kontroli w zakresie obowiązków formalnych i organizacyjnych. 67
2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych 69
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych 74
3.1. Wydawanie decyzji 74
3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa. 75
3.3. Rozpatrywanie skarg 77
3.3.1. Administracja publiczna 80
3.3.2. Bezpieczeństwo publiczne 82
3.3.3. Sądy, prokuratura, komornicy 83
3.3.4. Organizacje społeczne 84
3.3.5. Banki i inne instytucje finansowe 85

3.3.6. Internet 87
3.3.7. Marketing 89
3.3.8. Mieszkalnictwo 90
3.3.9. Oświata 92
3.3.10. Służba zdrowia 92
3.3.11. Ubezpieczenia społeczne, majątkowe i osobowe 93
3.3.12. Telekomunikacja 94
3.3.13. Zatrudnienie 95
3.3.14. Windykacja 96
3.3.15. Inne 97
4. Rozpatrywanie zawiadomień o naruszeniu danych osobowych 101
5. Egzekwowanie obowiązków o charakterze niepieniężnym określonych w decyzjach administracyjnych GIODO 102
6. Prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach 107
7. Rejestr zgłoszeń powołania administratora bezpieczeństwa informacji 121
8. Opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych 126
9. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych 181
9.1. Interpretacja przepisów 182
10. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych 244
10.5. Międzynarodowe konferencje, seminaria i spotkania 251
9.5. Wizyty robocze 254

Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2015 roku. 254

Część IV. Wnioski i planowane kierunki działań Generalnego Inspektora Ochrony Danych Osobowych 291

Załącznik nr 1. Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2015 o charakterze generalnym do centralnych organów państwa i do innych podmiotów z sektora publicznego 315

Załącznik nr 2. Wykaz kontroli przeprowadzonych w 2015 r. 318

Załącznik nr 3. Wykaz orzeczeń wydanych w 2015 r. przez Wojewódzki Sąd Administracyjny w Warszawie i Naczelny Sąd Administracyjny w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych..... 328
Załącznik nr 4. Informacje przekazane przez organy ścigania w sprawach zawiadomień o popełnieniu przestępstwa skierowanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2015 r. 346
Załącznik nr 5. Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych w 2015 r. 347
Załącznik nr 6. Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2015 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty 350
Załącznik nr 7. Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2015 r. za granicą..... 353

SPRAWOZDANIE Z DZIAŁALNOŚCI GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH W 2015 ROKU

Wprowadzenie

W dniu 9 kwietnia 2015 r. Sejm RP powołał na stanowisko Generalnego Inspektora Ochrony Danych Osobowych dr Edytę Bielak-Jomaa. Senat RP zaakceptował ten wybór 16 kwietnia 2015 r. Z chwilą złożenia ślubowania przed Sejmem nowo powołanego Generalnego Inspektora Ochrony Danych Osobowych, tj. od 22 kwietnia 2015 r., zgodnie z ustawą o ochronie danych osobowych, rozpoczęła się VI kadencja GIODO.

W okresie sprawozdawczym miała miejsce bardzo znacząca zmiana ram prawnych ochrony danych osobowych w Polsce. Otóż 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 (Dz. U. z 2014 r. poz. 1662), zmiany przepisów ustawy z dnia 29 sierpnia 1997 r. 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). Przyjęte rozwiązania, niezależnie od ich celu deregulacyjnego (zmniejszyły bowiem ilość obowiązków administratorów danych, którzy powołali ABI – zlikwidowano np. obowiązek zgłaszania zbiorów danych osobowych do GIODO w takim przypadku), miały również na celu przygotowanie administratorów danych do unormowań ogólnego rozporządzenia o ochronie danych stanowiącego część pakietu reform planowanych w UE w obszarze ochrony danych osobowych.

Część I. Źródła prawa w zakresie ochrony danych osobowych

1. Informacje ogólne

Prawo międzynarodowe. Najstarszym 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, która nałożyła na kraje członkowskie zobowiązanie stworzenia ustawodawstwa w zakresie ochrony danych osobowych, wskazując jednocześnie kierunek, w jakim ustawodawstwo to ma zmierzać. Celem Konwencji jest zapewnienie każdemu na obszarze państw członkowskich (niezależnie od obywatelstwa i zamieszkania) ochrony jego praw i wolności, a w szczególności prawa do poszanowania sfery osobistej, w związku z automatycznym przetwarzaniem danych osobowych. Konwencja Nr 108 została podpisana przez Polskę 24 kwietnia 1999 r. i ratyfikowana w maju 2002 r. (Dz. U. z 2003 r. Nr 3, poz. 25).

Prawo Unii Europejskiej. Początkowo Unia Europejska nie dostrzegała konieczności jednolitego uregulowania ochrony danych osobowych w aktach prawa krajowego. Komisja Europejska postulowała jedynie, aby państwa członkowskie ratyfikowały Konwencję Rady Europy 108. Z czasem jednak rozbieżności w ustawodawstwach państw Unii spowodowały konieczność ich ujednolicenia. Zasadniczym zadaniem, jaki taka regulacja miała spełnić było zapewnienie minimalnego, a zarazem wspólnego dla państw członkowskich poziomu ochrony danych osobowych gromadzonych w zbiorach oraz zapewnienie swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi. W 1990 r. rozpoczęto prace nad stosowną dyrektywą. Efektem tych prac było **wydanie Dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych**. Termin na jej implementację do porządków prawnych państw członkowskich wyznaczono na 23 października 1998 r. Do dziś wyznacza ona ramy prawne ochrony danych osobowych w Unii Europejskiej (Dz. Urz. WE L 281 z 23.11.1995).

Konstytucja Rzeczypospolitej Polskiej. Pierwsze gwarancje ochrony danych osobowych zapewniła w Polsce Konstytucja z 1997 r. Jej art. 47 zagwarantował każdemu prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (prawo do prywatności). Zgodnie zaś z art. 51, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Artykuł ten gwarantuje również każdemu prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych (ograniczenie tego prawa może określić ustawa) oraz prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub

zebranych w sposób sprzeczny z ustawą. Zasady i tryb gromadzenia oraz udostępniania informacji określać mogą wyłącznie przepisy rangi ustawy. Przepisem art. 51 Konstytucji zagwarantowana została autonomia informacyjna jednostki.

Ustawa o ochronie danych osobowych. Zasady ochrony danych ustanowione Dyrektywą 95/46/WE wprowadzone zostały do polskiego porządku prawnego **ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn. zm.).** Ustawa o ochronie danych osobowych wprowadziła szczegółowe normy służące ochronie danych osobowych w Polsce, a do dnia 1 maja 2004 r., czyli wstąpienia Polski do Unii Europejskiej, przeniosła do polskiego porządku prawnego wszystkie zasady określone w Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady. Przepisy ustawy obowiązują od dnia 30 kwietnia 1998 r.

Ustawa o ochronie danych osobowych określiła prawne ramy obrotu danymi osobowymi, a także zasady, jakie należy stosować przy przetwarzaniu danych osobowych. Sprecyzowała też prawa i obowiązki tzw. administratorów danych, m.in. organów, instytucji i osób prowadzących zbiory danych osobowych oraz prawa osób, których dane dotyczą, w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej oraz poszanowanie jej życia prywatnego.

Ustawa o ochronie danych osobowych, realizując wymagania stawiane przez prawo unijne, skonkretyzowała konstytucyjnie zagwarantowane prawo do decydowania o tym komu, w jakim zakresie i w jakim celu przekazujemy nasze dane osobowe, dając ustawowe gwarancje przestrzegania tego prawa poprzez wyposażenie osób, których dane dotyczą w środki służące realizacji tego prawa, a odpowiednie organy i służby w środki prawne, gwarantujące jego przestrzeganie. Podstawowym założeniem ustawy jest przyznanie każdej jednostce prawa do ochrony dotyczących jej danych.

Nad przestrzeganiem prawa obywateli do ochrony dotyczących ich danych osobowych czuwa Generalny Inspektor Ochrony Danych Osobowych - niezależny jednoosobowy organ 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 z późn. zm.);

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).

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 2014 r. poz. 1619 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.

Nie są to jedyne zadania należące do organu. Dodatkowe obowiązki GIODO wynikają również m.in. z **Dyrektywy 2002/58/WE o prywatności i łączności elektronicznej, Dyrektywy 2000/31/WE dotyczącej handlu elektronicznego, Decyzji ramowej 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych czy też Decyzji Rady nr 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiającej Europejski Urząd Policji (Europol).** W lipcu 2016 r. wejdzie w życie 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 (tzw. **rozporządzenie eIDAS**), które również będzie miało związek z nowymi zadaniami dla Generalnego Inspektora Ochrony Danych Osobowych.

Wskazane wyżej europejskie regulacje mają konkretne przełożenie na przepisy polskich aktów prawnych i funkcjonowanie Biura GIODO. Na mocy przepisów **ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne** (Dz. U. z 2014 r. poz. 243 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. W związku z powyższym, wyznaczeni przez Generalnego Inspektora pracownicy Biura GIODO wykonują zadanie organizacji i koordynacji przyjmowania oraz rozpatrywania zawiadomień o naruszeniu danych osobowych w oparciu o opracowaną instrukcję postępowania.

Ważny aspekt działalności organu wynika ponadto 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.). Zgodnie z art. 8 ust. 1 tej ustawy, Generalny Inspektor sprawuje kontrolę nad tym, czy wykorzystywanie danych (przetwarzanych w wyżej wskazanych systemach) nie narusza praw osób, których dane te dotyczą. W 2014 r. GIODO 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

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

2. Reforma prawa Unii Europejskiej w zakresie ochrony danych osobowych

Odpowiedzią na liczne problemy związane z zapewnieniem odpowiedniego poziomu ochrony danych osobowych oraz rozwój technologii związanych z ich przetwarzaniem, jak również coraz szersze pojmowanie pojęcia „dane osobowe" mają być nowe regulacje w tym zakresie. Obecnie na poziomie instytucji Unii Europejskiej negocjowana jest ostateczna wersja rozporządzenia w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych, które będzie bezpośrednio stosowane we wszystkich państwach członkowskich i uchyli dotychczas obowiązujące przepisy.

Projekt rozporządzenia – zaprezentowany przez Komisję 25 stycznia 2012 r. – przewidywał szereg istotnych zmian mających na celu wzmocnienie ochrony osób, których dane dotyczą. Uznano, że obecne ramy ochrony danych osobowych są nadmiernie rozdrobnione i skomplikowane z uwagi na fakt, iż Dyrektywa 95/46/WE została implementowana w różny sposób w poszczególnych państwach członkowskich. Komisarz ds. Wymiaru Sprawiedliwości i Obywatelstwa Viviane Reding, prezentując projekt, wskazywała na konieczność zastąpienia tego „morza biurokracji" jednym prawem, które będzie obowiązywało w całej Unii Europejskiej. Projekt ten przewiduje zastąpienie dyrektywy 95/46/WE **rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych**[2] oraz uchwalenie **dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania,**

[2] Wniosek Komisji Europejskiej COM (2012) 11 wersja ostateczna.

dochodzenia, wykrywania przestępstw i ścigania ich sprawców lub wykonywania sankcji karnych i swobodnego przepływu tych danych[3].

Najważniejsze propozycje zmian, jakie znalazły się w projekcie z 2012 r. obejmowały następujące rozwiązania:

- likwidację wymogów administracyjnych, takich jak obowiązek zgłaszania zbiorów danych do rejestracji organom nadzorującym ochronę danych – zamiast tego projekt przewiduje większą odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe (przykładowo przedsiębiorstwa i organizacje muszą powiadamiać krajowy organ nadzorczy o poważnych naruszeniach ochrony danych tak szybko, jak tylko jest to możliwe; jeżeli jest to wykonalne – w ciągu 24 godzin);
- administratorzy będą się kontaktować tylko z jednym krajowym organem nadzorującym ochronę danych w tym państwie członkowskim UE, w którym posiadają główną siedzibę. Również osoby fizyczne będą mogły kontaktować się z organem ochrony danych w swoim państwie, nawet jeżeli ich dane są przetwarzane przez przedsiębiorstwo mające siedzibę poza UE. W przypadku gdy do przetwarzania danych konieczna jest zgoda, zostało zastrzeżone, że będzie ona musiała zostać wyrażona w sposób wyraźny, a nie domniemany;
- „prawo do bycia zapomnianym" pomoże podmiotom danych lepiej zarządzać ryzykiem związanym z ochroną danych w Internecie: osoby fizyczne będą miały możliwość usunięcia swoich danych, jeżeli nie będzie istnieć uzasadniona podstawa do ich zachowania;
- unijne przepisy muszą obowiązywać w przypadku, gdy dane osobowe są przetwarzane za granicą przez przedsiębiorstwa prowadzące działalność na rynku UE i oferujące swoje usługi obywatelom UE;
- niezależne krajowe organy nadzorujące ochronę danych zostaną wzmocnione, aby mogły lepiej egzekwować unijne przepisy na terytorium kraju; zostaną one upoważnione do nakładania kar na przedsiębiorstwa naruszające unijne przepisy o ochronie danych;
- projekt Komisji Europejskiej obejmuje również wniosek ustawodawczy dotyczący dyrektywy w sprawie ochrony danych osobowych przetwarzanych na potrzeby zapobiegania, dochodzenia, wykrywania przestępstw i ścigania ich sprawców oraz

[3] Wniosek Komisji Europejskiej COM (2012) 10 wersja ostateczna.

powiązanych działań wymiaru sprawiedliwości w sprawach karnych. W nowej dyrektywie ogólne zasady ochrony danych zostaną zastosowane w odniesieniu do współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. Przepisy dyrektywy będą miały zastosowanie do przekazywania danych zarówno w kraju, jak i do transferów transgranicznych.

Zanim jednak przepisy rozporządzenia zaczną funkcjonować w praktyce, podczas dwuletniego okresu przejściowego państwa członkowskie będą miały obowiązek dostosowania krajowych przepisów do nowych, zmodernizowanych i uaktualnionych zasad ochrony danych osobowych. Oznacza to nie tylko konieczność zmiany przepisów polskiej ustawy o ochronie danych osobowych (która nie będzie mogła powtarzać regulacji zawartych w unijnym rozporządzeniu), ale także zrewidowania i ewentualnego przekształcenia przepisów dotyczących danych osobowych zawartych w innych aktach prawnych.

3. Biuro Generalnego Inspektora Ochrony Danych Osobowych

3.1. Struktura organizacyjna

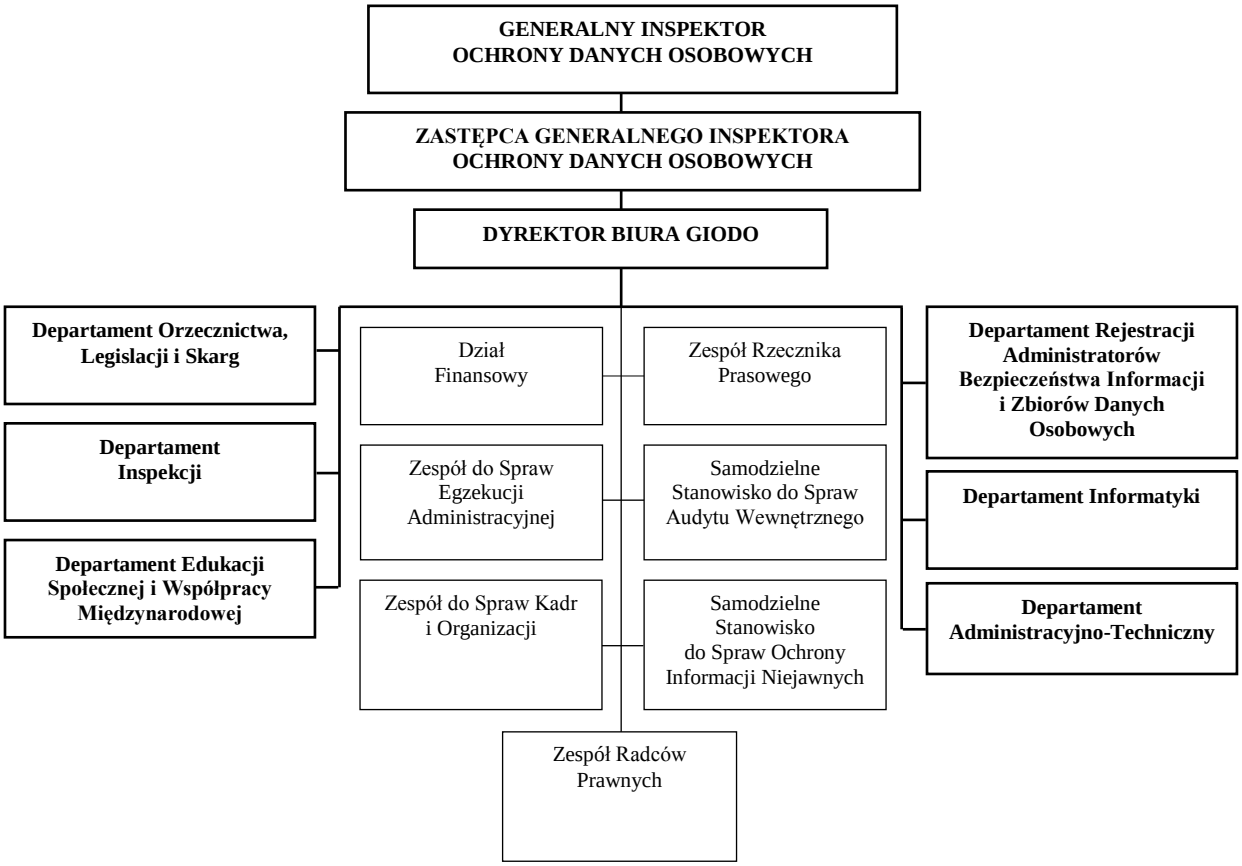
Zgodnie z art. 13 ust. 1 ustawy o ochronie danych osobowych, Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych. Tryb pracy Biura, a także organizację wewnętrzną i szczegółowy zakres zadań statutowych jednostek organizacyjnych oraz jednostek zamiejscowych 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 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 organizacyjna 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[4].

3.2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO w przeliczeniu na pełne etaty wynosił na dzień 1 stycznia 2015 r. – 126,105 etatów (tj. 129 osób), zaś na dzień 31 grudnia 2015 r. – **145,605** etatów (tj. 150 osób). Na stanowiskach merytorycznych zatrudnionych było 130 osób, a na stanowiskach pomocniczych 20 osób. Wyższe wykształcenie posiadało 131 pracowników, w tym 91 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2015 r. przedstawia się następująco:

- GIODO - 1 osoba (1 etat)
- Zastępca GIODO – 1 osoba (1 etat)
- Dyrektor Biura – 1 osoba (1 etat)
- Zespół Rzecznika Prasowego (ZRP) – 5 osób (5 etatów)
- Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) – 12 osób (11,75 etatu),
- Departament Informatyki (DIF) – 15 osób (14,50 etatów),
- Departament Inspekcji (DIS) – 15 osób (15 etatów),
- Departament Administracyjno-Techniczny (DAT) – 18 osób (17,40 etatu),
- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 48 osób (47,75 etatów),
- Departament Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych (DRZDO) – 19 osób (18,875 etatów),
- Dział Finansowy – 3 osoby (3 etaty),
- Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,25 etatu),
- Zespół ds. Kadr i Organizacji – 3 osoby (2,75 etatu),
- Samodzielne Stanowisko ds. Audytu – 1 osoba (0,33 etatu),
- Zespół Radców Prawnych – 3 osoby (2 etaty),

[4] 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.

- Zespół ds. Egzekucji Administracyjnej (ZEA) – 3 osoby (3 etaty).

3.3. Budżet Generalnego Inspektora Ochrony Danych Osobowych za 2015 r.

Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2015 r. wynosił: **16 749** tys. zł., w tym:

- wynagrodzenia	10 156,0 tys. zł
- pochodnie od wynagrodzeń	1 798,0 tys. zł
- wydatki majątkowe	736,0 tys. zł
- pozostałe wydatki	4 068,0 tys. zł

Wydatki zrealizowane przez GIODO w 2015 roku w kwocie **15 974,3** tys. zł obejmowały:

- wynagrodzenia	9 822,5 tys. zł
- pochodne od wynagrodzeń	1 645,7 tys. zł
- wydatki majątkowe	616,3 tys. zł
- pozostałe wydatki	3 889,8 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[5]. 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

[5] 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.

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.

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. 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 2015 r. Generalny Inspektor Ochrony Danych Osobowych przeprowadził łącznie **175 kontroli** zgodności przetwarzania danych osobowych z przepisami ustawy o ochronie danych osobowych, w tym skierował **13 wystąpień o dokonanie sprawdzeń przez administratorów bezpieczeństwa informacji (ABI).**

2.2.1. Administracja publiczna

W 2015 r. w podmiotach wykonujących zadania publiczne przeprowadzono **22 kontrole** zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W ramach tej kategorii podmiotów przeprowadzono kontrole 12 podmiotów przetwarzających dane osobowe w związku z realizacją zadań wynikających z przepisów ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2014 r. poz. 1863 z późn. zm.). Kontroli poddano ministra właściwego do spraw rodziny, jako administratora danych osobowych, Polską Wytwórnię Papierów Wartościowych S.A. z siedzibą w Warszawie oraz wybranych wójtów, burmistrzów i prezydentów miast wydających Karty Dużej Rodziny[6].

Minister Rodziny, Pracy i Polityki Społecznej realizując zadania wynikające z przepisów ustawy o Karcie Dużej Rodziny (zwanej dalej także: „Kartą"), polegające na zapewnieniu produkcji blankietów Kart, ich personalizacji i dystrybucji oraz zapewnieniu systemu teleinformatycznego, za pomocą którego są wykonywane czynności związane z realizacją ustawy o Karcie Dużej Rodziny, dokonał wyboru Polskiej Wytwórni Papierów Wartościowych S.A. (PWPW), jako podmiotu odpowiedzialnego za produkcję blankietów Kart, ich personalizację i dystrybucję, oraz jako podmiotu odpowiedzialnego za zapewnienie gminom (miastom) i Ministerstwu Rodziny, Pracy i Polityki Społecznej rozwiązania informatycznego umożliwiającego wprowadzanie przez wójtów (burmistrzów, prezydentów) do tego systemu danych członków rodzin wielodzietnych i udostępnianie niezbędnych danych z tego systemu PWPW w celu personalizacji Kart i ich dystrybucji do organów przyznających Karty celem ich wydania członkom rodzin wielodzietnych.

Umowa zawarta pomiędzy Ministerstwem Rodziny, Pracy i Polityki Społecznej a Polską Wytwórnią Papierów Wartościowych S.A. spełniała wymagania umowy powierzenia

[6] Np. kontrole DIS-K-421/107/15, DIS-K-421/115/15, DIS-K-421/120/15 i DIS-K-421/128/15.

przetwarzania danych osobowych. Zgodnie z § 8 ww. umowy, Minister Rodziny, Pracy i Polityki Społecznej powierzał Polskiej Wytwórni Papierów Wartościowych S.A. przetwarzanie danych osobowych w zbiorze o nazwie „Karta Dużej Rodziny" zgłoszonym Generalnemu Inspektorowi i przez niego zarejestrowanym. Kontrola przeprowadzona w Ministerstwie Rodziny, Pracy i Polityki Społecznej wykazała, iż Minister nie posiadał dostępu do danych osobowych członków rodzin wielodzietnych, którym wydane zostały Karty Dużej Rodziny przetwarzanych zarówno w zapisie papierowym, jak i w systemie informatycznym. Danych tych nie pozyskiwał także w żadnym innym celu od podmiotu, któremu powierzył przetwarzanie danych osobowych, tj. Polskiej Wytwórni Papierów Wartościowych S.A. W systemie informatycznym Minister Rodziny, Pracy i Polityki Społecznej posiadał wyłącznie dostęp do danych statystycznych dotyczących członków rodzin wielodzietnych (np. liczby wydanych Kart czy złożonych wniosków o przyznanie Karty).

Kartę Dużej Rodziny przyznaje wójt (prezydent, burmistrz) właściwy ze względu na miejsce zamieszkania członka rodziny wielodzietnej. Kontrola wykazała, iż w dwóch przypadkach organ gminy upoważnił pracownika urzędu gminy (miasta) do realizacji zadań wynikających z ustawy o Karcie Dużej Rodziny, natomiast w czterech przypadkach upoważnił do realizacji ww. zadań kierownika jednostki organizacyjnej gminy. Przesłankę przetwarzania przez Ministra Rodziny, Pracy i Polityki Społecznej danych osobowych członków rodziny wielodzietnej, w związku z przyznaniem Karty Dużej Rodziny, stanowi art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych[7]. Przepisami takimi są m.in.: ustawa o Karcie Dużej Rodziny oraz rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 23 grudnia 2014 r. w sprawie sposobu unieważnienia Karty Dużej Rodziny, wzorów graficznych oraz wzoru wniosku w sprawie przyznania Karty Dużej Rodziny (Dz. U. z 2014 r. poz. 1954 z późn. zm.). Administratorami danych osobowych przetwarzanych w zakresie niezbędnym do realizacji zadań wynikających z ustawy o Karcie Dużej Rodziny są wójt (burmistrz, prezydent) oraz Minister Rodziny, Pracy i Polityki Społecznej, stosownie do art. 21 ust. 2 ustawy o Karcie Dużej Rodziny[8]. Czynności kontrolne przeprowadzone w Ministerstwie Rodziny, Pracy i Polityki Społecznej oraz w Polskiej Wytwórni Papierów Wartościowych S.A. nie wykazały w zakresie objętym kontrolą uchybień w procesie przetwarzania danych osobowych, tj. w zakresie niezbędnym do realizacji zadań

[7] Art. 23.1.2. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

[8] Art. 21.2. Administratorami danych osobowych przetwarzanych w zakresie niezbędnym do realizacji zadań wynikających z niniejszej ustawy są wójt oraz minister właściwy do spraw rodziny.

wynikających z przepisów ustawy o Karcie Dużej Rodziny oraz w związku z zawartą umową pomiędzy Ministerstwem Rodziny, Pracy i Polityki Społecznej a Polską Wytwórnią Papierów Wartościowych S.A., dotyczącą realizacji zadań wynikających z przepisów ustawy o Karcie Dużej Rodziny. Stwierdzono natomiast uchybienia w organach samorządu terytorialnego przyznających Kartę Dużej Rodziny. Uchybienia te polegały w szczególności na nieuwzględnieniu w dokumentacji składającej się na politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, informacji dotyczących przetwarzania danych w zbiorze o nazwie „Karta Dużej Rodziny" z wykorzystaniem systemu informatycznego, niezamieszczeniu w prowadzonej ewidencji osób upoważnionych do przetwarzania danych osobowych wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych oraz niezgłoszeniu zbioru danych o nazwie „Karta Dużej Rodziny" do rejestracji Generalnemu Inspektorowi.

Wobec organów przyznających Kartę Dużej Rodziny, 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[9].

2.2.2. Bezpieczeństwo publiczne

W 2015 r. Generalny Inspektor przeprowadził **16 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 jednostkach Policji, w Straży Granicznej, wydziałach (referatach) konsularnych przy ambasadach Rzeczypospolitej Polskiej oraz w Ministerstwie Spraw Zagranicznych i Ministerstwie Sprawiedliwości**[10]. 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

[9] Np. decyzje nr DIS/DEC-975/15/107720, DIS/DEC-991/15/107973.

[10] Np. kontrole DIS-K-421/76/15, DIS-K-411/119/15, DIS-K-411/129/15, DIS-K-411/162/15, DIS-K-421/206/15.

Wizowym Systemie Informacyjnym (Dz. U. z 2014 r. poz. 1203 z późn. zm.), tj. wglądu w dane SIS i dane VIS oraz dokonywania wpisów danych SIS i danych VIS.

Wizowy System Informacyjny (VIS) został ustanowiony na mocy art. 1 decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS). Celem VIS, stosownie do postanowień rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz. Urz. UE L z 2008 r. Nr 218/60), jest poprawa realizacji wspólnej polityki wizowej, poprawa współpracy konsularnej i procesu konsultacji pomiędzy centralnymi organami wizowymi poprzez ułatwienie wymiany danych pomiędzy państwami członkowskimi o wnioskach i związanych z nimi decyzjach, w szczególności w celu uproszczenia procedury składania wniosków wizowych, ułatwienia odpraw w przejściach granicznych na granicach zewnętrznych państw członkowskich i na terytorium państw członkowskich, pomocy w identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium państw członkowskich lub też przestały spełniać te warunki oraz przyczynienia się do zapobiegania zagrożeniom bezpieczeństwa wewnętrznego każdego z państw członkowskich. Natomiast System Informacyjny Schengen drugiej generacji (SIS II) został utworzony na mocy 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 decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II). Celem SIS II, stosownie do postanowień ww. aktów prawnych, jest zapewnienie przy wykorzystaniu informacji przekazywanych za pośrednictwem tego systemu, wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej, w tym utrzymywanie bezpieczeństwa publicznego oraz porządku publicznego oraz zagwarantowanie bezpieczeństwa na terytorium państw członkowskich. Zasady i sposób realizacji udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, w tym obowiązki i uprawnienia organów dotyczące dokonywania wpisów oraz wglądu do danych zawartych w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, zostały określone w ustawie 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.).

Przeprowadzone kontrole wykazały, że organy i służby uprawnione do dostępu do danych SIS i danych VIS dostęp ten uzyskują albo poprzez własny system informatyczny (system instytucjonalny) albo za pośrednictwem aplikacji WWW SIS i WWW VIS. Osobom mającym dostęp do danych SIS i danych VIS nadane zostały upoważnienia dla użytkownika indywidualnego do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych (w przypadku, gdy dostęp do tych danych jest uzyskiwany poprzez aplikacje WWW SIS i WWW VIS), upoważnienia dla użytkownika końcowego (w przypadku, gdy dostęp do tych danych uzyskiwany jest poprzez system instytucjonalny organu), a także upoważnienia do przetwarzania danych osobowych. Ww. osoby odbyły szkolenie z zakresu bezpieczeństwa i ochrony danych oraz otrzymały zaświadczenia potwierdzające odbycie takiego szkolenia.

Do istotnych kontroli w tym zakresie należała kontrola przeprowadzona w Ministerstwie Sprawiedliwości[11], w związku z dostępem do danych SIS, wprowadzanych przez poszczególne sądy okręgowe i sądy apelacyjne, jaki posiada Minister Sprawiedliwości z uwagi na utrzymywanie systemu informatycznego umożliwiającego sądom dostęp do tych danych. Jak wskazano w toku kontroli, dostęp do danych SIS w Ministerstwie Sprawiedliwości był związany z realizacją dyspozycji wynikającej z ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2015 r. poz. 133 z późn. zm.), zgodnie z którą nadzór administracyjny nad działalnością sądów sprawuje Minister Sprawiedliwości (art. 9 tej ustawy). Jak ustalono w toku kontroli, Minister Sprawiedliwości posiadał pełen wgląd do danych SIS, mógł dokonywać zmiany lub usunięcia danych SIS, jednak takich czynności nie realizował. W związku z dokonanymi ustaleniami powstała wątpliwość, co do podstaw prawnych dostępu do danych SIS przez Ministra Sprawiedliwości. Minister Sprawiedliwości nie został bowiem wymieniony w ustawie o udziale Rzeczpospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym jako organ uprawniony do dostępu do tych danych. Zdaniem Ministra Sprawiedliwości, taka podstawa może natomiast wynikać z przepisów 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

[11] Kontrola DIS-K-421/36/15

generacji (SIS II) (Dz. Urz. UE L 381 z 28.12.2006, str. 4) i decyzji Rady nr 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 2007.205.63), które odpowiednio w art. 27 ust. 2[12] i art. 40 ust. 2[13] przyznają dostęp do danych SIS podmiotom pełniącym funkcje koordynujące. Wskazana kwestia pozostaje przedmiotem analizy Generalnego Inspektora Ochrony Danych Osobowych.

Pozostałe kontrole przeprowadzone w podmiotach mających dostęp do danych SIS i / lub danych VIS w większości przypadków nie wykazały uchybień w zakresie przestrzegania przepisów ochronie danych osobowych. Jedynie w przypadku jednostek Straży Granicznej oraz wydziałów (referatów) konsularnych ambasad RP i Ministerstwa Spraw Zagranicznych stwierdzono pojedyncze naruszenia przepisów odnoszących się do przetwarzania danych osobowych w związku z dostępem do danych SIS i danych VIS. W przypadku Straży Granicznej uchybienie polegało na braku kontroli działań użytkowników mającej na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami, o której mowa w art. 24 ustawy o udziale Rzeczpospolitej Polskiej w Systemie Informacji Schengen oraz Wizowym Systemie Informacyjnym[14], w sytuacji gdy dostęp do danych SIS następował przy wykorzystaniu aplikacji WWW SIS, a do danych VIS przy wykorzystaniu aplikacji WWW VIS. Jak bowiem ustalono w toku kontroli, Komenda Główna Straży Granicznej nie występowała do Centralnego Organu Technicznego KSI o udostępnienie logów zdarzeń dotyczących użytkowników indywidualnych, co jest niezbędne do zapewnienia takiej kontroli. Natomiast w toku kontroli wydziałów (referatów) konsularnych ambasad RP i Ministerstwa Spraw Zagranicznych ustalono, że w wykazie budynków i lokali stanowiących obszar przetwarzania danych osobowych, będącym elementem polityki bezpieczeństwa, nie

[12] Art. 27.2 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) (Dz. Urz. UE L 381 z 28.12.2006, str. 4). Prawo dostępu do danych wprowadzonych do SIS II oraz prawo do bezpośredniego przeszukiwania takich danych mogą być wykonywane również przez krajowe organy sądownicze, w tym odpowiedzialne za wszczynanie dochodzeń z oskarżenia publicznego w postępowaniu karnym i dochodzeń sądowych przed wniesieniem aktu oskarżenia, w ramach wykonywania zadań określonych przez ustawodawstwo krajowe, a także przez organy pełniące wobec nich funkcję koordynującą.

[13] Art. 40.2 decyzji Rady nr 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 2007.205.63). Prawo dostępu do danych wprowadzonych do SIS II oraz prawo do bezpośredniego przeszukiwania takich danych mogą być wykonywane również przez krajowe organy sądowe - w tym organy odpowiedzialne za wszczynanie dochodzeń z oskarżenia publicznego w postępowaniu karnym i dochodzeń sądowych przed wniesieniem aktu oskarżenia, w ramach wykonywania zadań określonych przez ustawodawstwo krajowe - a także przez organy pełniące wobec nich funkcje koordynującą.

[14] Art. 24. Organ uprawniony do wykorzystywania danych poprzez Krajowy System Informatyczny (KSI) jest obowiązany stosować odpowiednie procedury kontrolne wskazujące działania podejmowane w ramach danego organu mające na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami.

zostały ujęte niektóre punkty wizowe, gdzie były przyjmowane od interesantów wnioski wizowe oraz aktualny adres wydziału konsularnego jednej z ambasad RP, a w wykazie zbiorów danych osobowych przetwarzanych w Ministerstwie Spraw Zagranicznych oraz placówkach zagranicznych, będącym również elementem polityki bezpieczeństwa, nie uwzględniono aplikacji WWW SIS i WWW VIS.

Uchybienia stwierdzono również w niektórych kontrolach przeprowadzonych w jednostkach Policji. Jak bowiem ustalono w toku tych kontroli, dostęp do danych SIS wykorzystywany był także przy sporządzaniu opinii o osobie w sprawach dotyczących wydawania pozwoleń na broń palną oraz przy wydawaniu postanowień dotyczących opinii o osobie w sprawach dotyczących wpisu na listę kwalifikowanych pracowników ochrony fizycznej oraz wpisu na listę kwalifikowanych pracowników zabezpieczenia technicznego, a więc w przypadkach nieprzewidzianych w przepisach ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Zasadność dostępu do danych SIS w ww. przypadkach będzie przedmiotem analizy Generalnego Inspektora.

W związku z funkcjonowaniem systemu informatycznego o nazwie „Eurodac" przeprowadzono w 2015 r. trzy kontrole[15] zgodności przetwarzania danych z przepisami o ochronie danych osobowych w: Urzędzie do Spraw Cudzoziemców (UdSC)[16], Straży Granicznej[17] oraz w Centralnym Laboratorium Kryminalistycznym Policji (CLKP)[18].

System Eurodac do dnia 19 lipca 2015 r. funkcjonował na podstawie rozporządzenia Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej (Dz. Urz. UE L z 2000 r. Nr 316/1). Od 20 lipca 2015 r. zasady funkcjonowania ww. systemu określa rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 26 czerwca 2013 r. nr 603/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską

[15] Kontrole DIS-K-421/67/15, DIS-K-421/103/15, DIS-K-421//15.
[16] DIS-K-421/67/15
[17] DIS-K-421/118/15
[18] DIS-K-421/103/15

Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz. Urz. UE L z 2013 r. Nr 180/1) – dalej rozporządzenie 603/2013.

Celem systemu Eurodac jest:

1) pomoc w ustalaniu, które państwo członkowskie, zgodnie z rozporządzeniem (UE) nr 604/2013, odpowiada za rozpatrywanie wniosków o ochronę międzynarodową złożonych w państwie członkowskim przez obywatela państwa trzeciego lub bezpaństwowca, a także ułatwianie w inny sposób stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (Dz.U.UE.L.2013.180.31) - dalej rozporządzenie 604/2013 tzw. Dublin III; na warunkach określonych w niniejszym rozporządzeniu 604/2013;

2) określenie warunków, na jakich wyznaczone organy państw członkowskich oraz Europejski Urząd Policji (Europol) mogą występować z wnioskiem o porównanie danych daktyloskopijnych z danymi przechowywanymi w systemie centralnym na potrzeby ochrony porządku publicznego;

3) bez uszczerbku dla możliwości przetwarzania danych przeznaczonych do Eurodac przez państwo członkowskie pochodzenia w bazach danych ustanowionych na mocy prawa krajowego tego państwa członkowskiego, dane daktyloskopijne i inne dane osobowe mogą być przetwarzane w Eurodac tylko w celach określonych w niniejszym rozporządzeniu oraz w art. 34 ust. 1 rozporządzenia (UE) nr 604/2013[19].

[19] Zgodnie z art. 34 ust. 1 rozporządzenia (UE) nr 604/2013: 1. Każde państwo członkowskie przekazuje wszystkim państwom członkowskim, które się o to zwrócą, dane osobowe dotyczące wnioskodawcy, które są odpowiednie, właściwe, i wystarczające do: a) ustalenia odpowiedzialnego państwa członkowskiego; b) rozpatrzenia wniosku o udzielenie ochrony międzynarodowej; c) wykonania wszelkich zobowiązań wynikających z niniejszego rozporządzenia. 2. Informacje, o których mowa w ust. 1, mogą obejmować wyłącznie: a) dane identyfikacyjne wnioskodawcy oraz, w odpowiednich przypadkach, członków jego rodziny, krewnych lub innych osób należących do rodziny (imię i nazwisko oraz, w odpowiednim przypadku, poprzednie nazwisko, przydomki lub pseudonimy; obywatelstwo, obecne i poprzednie; data i miejsce urodzenia); b) dokumenty tożsamości i dokumenty podróży (numery referencyjne, okres ważności, data wydania, organ wydający, miejsce wydania itd.); c) inne informacje niezbędne dla ustalenia tożsamości wnioskodawcy, w tym odciski palców przetwarzane zgodnie z rozporządzeniem (UE) nr 603/2013; d) miejsca zamieszkania oraz trasy odbytych podróży; e) dokumenty pobytu lub wizy wydane przez państwo członkowskie; f) miejsce złożenia wniosku; g) datę złożenia wszelkich poprzednich wniosków o udzielenie ochrony międzynarodowej, datę złożenia obecnego wniosku, etap, na którym znajduje się postępowanie, i ewentualnie podjętą decyzję. 3. Ponadto, pod warunkiem że jest to niezbędne dla rozpatrzenia wniosku o udzielenie ochrony międzynarodowej, odpowiedzialne państwo członkowskie może zwrócić się do innego państwa członkowskiego o powiadomienie go, na jakiej podstawie wnioskodawca opiera swój wniosek oraz, w odpowiednich przypadkach, jakie są podstawy wszelkich podjętych decyzji dotyczących wnioskodawcy. Inne państwo członkowskie może odmówić

Zgodnie z art. 3 rozporządzenia 603/2013 na system Eurodac składają się:

a) skomputeryzowana centralna baza danych daktyloskopijnych ("system centralny") złożona z jednostki centralnej, planu i systemu zachowania ciągłości działania;

b) infrastruktura łączności między systemem centralnym a państwami członkowskimi, zapewniająca szyfrowaną wirtualną sieć służącą do przekazywania danych Eurodac ("infrastruktura łączności").

---

odpowiedzi na przedłożony mu wniosek, jeżeli przekazanie takich informacji przypuszczalnie zaszkodziłoby jego ważnym interesom lub ochronie swobód i praw i podstawowych osoby, której informacje dotyczą, lub innych osób. W każdym przypadku przekazanie wnioskowanych informacji wymaga uzyskania przez wnioskujące państwo członkowskie pisemnej zgody osoby ubiegającej się o ochronę międzynarodową. W takim przypadku wnioskodawca musi wiedzieć, jakich informacji dotyczy wyrażana zgoda. 4. Wszelkie wnioski o udzielenie informacji są wysyłane wyłącznie w kontekście konkretnego wniosku o udzielenie ochrony międzynarodowej. We wniosku podawane są podstawy, na których został oparty, oraz w przypadku gdy ma on na celu sprawdzenie, czy istnieje kryterium mogące pociągać za sobą odpowiedzialność państwa członkowskiego, do którego wniosek jest kierowany, podawane są także dowody, w tym istotne informacje z wiarygodnych źródeł o sposobach i środkach wjazdu na terytorium państwa członkowskiego wnioskodawców lub konkretny i możliwy do zweryfikowania fragment oświadczeń wnioskodawcy, na których wniosek został oparty. Przyjmuje się, że takie istotne informacje z wiarygodnych źródeł są same w sobie niewystarczające do ustalenia odpowiedzialności i kompetencji państwa członkowskiego na podstawie niniejszego rozporządzenia, ale mogą pomóc w ocenie innych przesłanek odnoszących się do poszczególnych wnioskodawców. 5. Państwo członkowskie, do którego skierowano wniosek, udziela odpowiedzi w terminie pięciu tygodni. Wszelkie opóźnienia w udzieleniu odpowiedzi są należycie uzasadniane. Niedotrzymanie terminu pięciu tygodni nie zwalnia państwa członkowskiego, do którego skierowano wniosek, z obowiązku udzielenia odpowiedzi. Jeżeli w wyniku badań przeprowadzonych przez państwo członkowskie, do którego skierowano wniosek i które przekroczyło maksymalny termin, uzyskane zostaną informacje wskazujące, że jest ono odpowiedzialnym państwem członkowskim, to państwo członkowskie nie może powoływać się na przekroczenie terminów przewidzianych w art. 21, 23 i 24 jako przyczynę odmowy uwzględnienia wniosku o przejęcie lub wtórne przejęcie. W takim przypadku terminy przewidziane w art. 21, 23 i 24 na złożenie wniosku o przejęcie lub wtórne przejęcie przedłuża się o okres równy zwłoce w udzieleniu odpowiedzi przez państwo członkowskie, do którego skierowano wniosek. 6. Wymiana informacji przeprowadzana jest na wniosek państwa członkowskiego i może odbywać się jedynie między organami, o których wyznaczeniu przez każde państwo członkowskie powiadomiono Komisję zgodnie z art. 35 ust. 1. 7. Informacje uzyskane w ramach wymiany mogą być wykorzystywane jedynie do celów określonych w ust. 1. W każdym państwie członkowskim takie informacje mogą być, w zależności od ich rodzaju i uprawnień organu otrzymującego, przekazywane jedynie organom i sądom, którym powierzono: a) ustalenie odpowiedzialnego państwa członkowskiego; b) rozpatrzenie wniosku o udzielenie ochrony międzynarodowej; c) wykonanie wszelkich zobowiązań wynikających z niniejszego rozporządzenia. 8. Państwo członkowskie, które przekazuje informacje, zapewnia, że są one dokładne i aktualne. Jeżeli okaże się, że przekazało ono informacje niedokładne lub informacje, które nie powinny były zostać przekazane, państwa członkowskie będące odbiorcami tych informacji zostają o tym natychmiast powiadomione. Są one zobowiązane do poprawienia lub usunięcia tych informacji. 9. Wnioskodawca ma prawo do uzyskania na żądanie informacji o wszelkich przetwarzanych danych, które go dotyczą. Jeżeli wnioskodawca stwierdzi, że dane te były przetwarzane z naruszeniem niniejszego rozporządzenia lub dyrektywy 95/46/WE, w szczególności z tego względu, że są one niekompletne lub niedokładne, jest on uprawniona do żądania ich poprawienia lub usunięcia. Organ, który poprawia lub usuwa te dane, powiadamia, w zależności od przypadku, państwo członkowskie przekazujące lub otrzymujące informacje. Wnioskodawca ma prawo wnieść powództwo lub skargę do właściwych organów lub sądów państwa członkowskiego, które odmówiło mu prawa dostępu do danych go dotyczących lub prawa do poprawienia lub usunięcia tych danych. 10. W każdym zainteresowanym państwie członkowskim odnotowuje się w indywidualnych aktach zainteresowanej osoby lub w rejestrze fakt przekazania i otrzymania wymienianych informacji. 11. Dane uzyskane w ramach wymiany przechowywane są przez okres nieprzekraczający okresu niezbędnego do realizacji celów, dla których są one wymieniane. 12. W przypadku gdy dane nie są przetwarzane automatycznie lub nie są albo nie mają być zawarte w aktach, każde państwo członkowskie podejmuje właściwe środki w celu zapewnienia zgodności z niniejszym artykułem przez skuteczne kontrole.

Każde państwo członkowskie posiada jeden krajowy punkt dostępu (tj. wyznaczony system krajowy, który komunikuje się z systemem centralnym). W przypadku Polski ww. punktem jest system AFIS (Automatyczny System Identyfikacji Daktyloskopijnej) obsługiwany przez Centralne Laboratorium Kryminalistyczne Policji[20].

Dane osób objętych art. 9 ust. 1, art. 14 ust. 1 i art. 17 ust. 1 rozporządzenia 603/2013, znajdujące się w systemie centralnym, są przetwarzane w imieniu państwa członkowskiego pochodzenia na warunkach określonych w rozporządzeniu 603/2013 oraz rozdzielane za pomocą odpowiednich środków technicznych. Przepisy regulujące działanie systemu Eurodac mają również zastosowanie do operacji przeprowadzanych przez państwa członkowskie, począwszy od przesłania danych do systemu centralnego aż do wykorzystania wyników porównania.

Z danych zawartych w systemie Eurodac w Polsce korzystają w szczególności Urząd do Spraw Cudzoziemców, Straż Graniczna, natomiast Centralne Laboratorium Kryminalistyczne Policji (CLKP) zapewnia tym organom techniczny dostęp do systemu Eurodac.

Do zadań CLKP należy utrzymanie, prowadzenie i rozwój wykrywczych baz danych, tj. Centralnej Registratury Daktyloskopijnej (dalej również CRD) wraz z Automatycznym Systemem Identyfikacji Daktyloskopijnej (system AFIS) oraz Krajowym Punktem Kontaktowym Eurodac (NAP).

W ramach realizowanych zadań CLKP prowadzi zbiór danych o nazwie „Centralna Registratura Daktyloskopijna", na który składają się między innymi karty daktyloskopijne cudzoziemców prowadzone w formie papierowej. Karty daktyloskopijne podzielone są wg celu ich sporządzenia i wykorzystania: tj. 1) cel związany z ochroną porządku publicznego (wykrywczych i identyfikacyjnych) oraz 2) cele administracyjne. Źródłem kart daktyloskopijnych gromadzonych dla celów wykrywczych i identyfikacyjnych są: Policja, Straż Graniczna, Żandarmeria Wojskowa oraz organy wskazane w umowach międzynarodowych. Natomiast źródłem kart daktyloskopijnych cudzoziemców gromadzonych dla celów administracyjnych jest Straż Graniczna oraz Policja. Utworzenie zbioru kart daktyloskopijnych dla celów administracyjnych było związane z realizacją przepisów rozporządzenia Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego

[20] DIS-K-421/103/15

stosowania Konwencji Dublińskiej), a obecnie jego prowadzenie jest związane z realizacją przepisów rozporządzenia Nr 603/2013, w zakresie celów określonych w art. 1 ust. 1.

Karty daktyloskopijne są przechowywane w CRD z podziałem na dwa podzbiory: kryminalny (Zbiór Rejestracji Kryminalnych) i administracyjny (Zbiór Rejestracji Administracyjnych).

Wszystkie papierowe karty daktyloskopijne cudzoziemców przechowywane przez CLKP posiadają swój odpowiednik w formie cyfrowej w systemie informatycznym o nazwie AFIS. Celem przetwarzania przez CLKP danych zawartych w kartach daktyloskopijnych zgromadzonych w Zbiorze Rejestracji Administracyjnych (karty daktyloskopijne cudzoziemców gromadzone dla celów administracyjnych), stanowiącym część zbioru danych o nazwie „Centralna Registratura Daktyloskopijna", jest administrowanie tym zbiorem danych oraz udostępnianie informacji z tego rejestru organom wskazanym w art. 450 ust. 1 pkt 1 i pkt 2 ustawy o cudzoziemcach[21]. Udostępnienie danych z tego zbioru następuje wyłącznie na pisemny wniosek uprawnionego organu.

Karty daktyloskopijne cudzoziemca są sporządzane przez Straż Graniczną lub w wyjątkowych przypadkach przez Policję za pomocą urządzenia LiveScanner lub tradycyjnie metodą tuszową w związku z: ubieganiem się przez cudzoziemca o ochronę międzynarodową (kategoria 1); zatrzymaniem cudzoziemca w związku z nielegalnym przekroczeniem granicy zewnętrznej (kategoria 2); zatrzymaniem cudzoziemca w związku z nielegalnym pobytem na terytorium RP (kategoria 3); wystąpieniem przez cudzoziemca z wnioskiem o uzyskanie informacji o danych, którego go dotyczą, zapisanych w systemie Eurodac, na podstawie art. 29 ust. 4 i 5 rozporządzenia Nr 603/2013 (kategoria 9).

Wysyłając zapytania do Systemu Centralnego Eurodac, CLKP działa jako Krajowy Punkt Dostępu do systemu Eurodac (NAP Eurodac), do pełnienia roli którego zostało wyznaczone zgodnie z art. 3 ust. 2 rozporządzenia Nr 603/2013[22].

[21] Dane przetwarzane w krajowym zbiorze rejestrów, ewidencji i wykazu w sprawach cudzoziemców, o których mowa w art. 449 ust. 2 pkt 1-12 i 16, udostępnia się następującym podmiotom, w zakresie niezbędnym do realizacji ich ustawowych zadań: 1) organom administracji publicznej, sądom i prokuraturom; 2) Radzie do Spraw Uchodźców, Policji, Straży Granicznej, Służbie Więziennej, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Służbie Celnej, Żandarmerii Wojskowej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Biuru Ochrony Rządu, Państwowej Inspekcji Pracy, Centralnemu Biuru Antykorupcyjnemu, Szefowi Krajowego Centrum Informacji Kryminalnych i straży gminnej (miejskiej).

[22] Informacja o wyznaczeniu CLKP do pełnienia roli krajowego punktu dostępu do systemu Eurodac została zamieszczona w Dzienniku Urzędowym Unii Europejskiej z dnia 20 lipca 2015 r. (Dz. Urz. UE L z 2015/C 237/01).

Ponadto w związku z funkcjonowaniem systemu Eurodac, CLKP pełni rolę organu weryfikującego dla Policji w odniesieniu do celów określonych w art. 1 ust. 2 rozporządzenia Nr 603/2013[23]. Wszystkie czynności wykonywane przez CLKP w ramach systemu Eurodac są realizowane na zlecenie innych podmiotów, tj. dla celu określonego w art. 1 ust. 1 rozporządzenia Nr 603/2013 – na zlecenie Szefa Urzędu do Spraw Cudzoziemców, Rady ds. Uchodźców, Straży Granicznej, Policji oraz Systemu Centralnego Eurodac, natomiast dla celu określonego w art. 1 ust 2 ww. rozporządzenia – na zlecenie Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Policji oraz Centralnego Biura Antykorupcyjnego.

W toku kontroli przeprowadzonej w jednej z placówek Straży Granicznej ustalono, że do jej zadań należy m.in. przyjmowanie wniosków o nadanie statusu uchodźcy na terytorium RP, jak również prowadzenie postępowań administracyjnych w sprawie zobowiązywania cudzoziemców do powrotu w przypadkach i na zasadach określonych w ustawie o cudzoziemcach.

W ramach realizacji ww. zadań placówka pobiera odciski palców od osób ubiegających się o ochronę międzynarodową na terytorium Rzeczypospolitej Polskiej (kategoria 1 Eurodac), zgodnie z wymogami rozporządzenia nr 603/2013. Wniosek o nadanie statusu uchodźcy składa się do Szefa Urzędu do Spraw Cudzoziemców za pośrednictwem komendanta oddziału lub komendanta placówki Straży Granicznej.

Do systemu Eurodac przekazywane są dane daktyloskopijne - odciski wszystkich palców – każdej osoby objętej wnioskiem o nadanie statusu uchodźcy w wieku co najmniej 14 lat. Cudzoziemcom, którzy deklarują chęć złożenia wniosku o nadanie statusu uchodźcy, przekazywana jest ulotka informacyjna na temat zasad rozpatrywania wniosków o nadanie statusu uchodźcy oraz praw i obowiązków cudzoziemców ubiegających się o nadanie statusu uchodźcy, informacja na temat tzw. postępowań dublińskich oraz wykaz instytucji udzielających pomocy uchodźcom. Informacje te są przekazywane cudzoziemcowi w zrozumiałym dla niego języku. Przed pobraniem odcisków linii papilarnych od osoby ubiegającej się o nadanie statusu uchodźcy, w każdym przypadku osoba taka otrzymuje na piśmie lub, w razie konieczności, ustnie w znanym jej w języku, pouczenie o podstawach prawnych daktyloskopowania oraz przysługujących jej prawach w związku z rejestracją jej danych w systemie Eurodac. Funkcjonariusze placówki pobierają za pomocą urządzenia LiveScanner lub ewentualnie metodą tuszową odciski wszystkich palców od wszystkich osób

[23] O fakcie wyznaczenia CLKP do pełnienia roli organu weryfikującego dla Policji została poinformowana Komisja Europejska w informacji Ministra Spraw Wewnętrznych z dnia 27 października 2014 r.

objętych wnioskiem o nadanie statusu uchodźcy, które ukończyły 14 rok życia i sporządzają za pomocą tego urządzenia karty daktyloskopijne cudzoziemca. Odciski linii papilarnych cudzoziemców, którzy ubiegają się o nadanie statusu uchodźcy są pobierane niezwłocznie po przyjęciu wniosku o nadanie statusu uchodźcy. Pobrane odciski palców oraz wprowadzone przez funkcjonariusza dane osoby ubiegającej się o nadanie statusu uchodźcy są przesyłane za pośrednictwem systemu informatycznego do CLKP w celu ich zarejestrowania w systemie AFIS oraz w celu przekazania danych wskazanych w art. 11 rozporządzenia nr 603/2013 do systemu centralnego Eurodac. W przypadku osób ubiegających się o nadanie statusu uchodźcy, ich dane daktyloskopijne są zapisywane zarówno w systemie centralnym Eurodac jak i w systemie AFIS.

Następnie placówka kieruje sprawę do Szefa UdSC w celu jej rozpatrzenia. Wypełniony wniosek o nadanie statusu uchodźcy wraz z paszportem, kserokopią karty daktyloskopijnej cudzoziemca i pozostałymi dokumentami zgromadzonymi w sprawie, są dostarczane przez upoważnionego funkcjonariusza placówki do UdSC. W sytuacji, gdy placówka przesyła odciski palców cudzoziemca do systemu Eurodac w celu ich porównania z danymi Eurodac, wynik tego porównania otrzymuje CLKP, które wprowadza uzyskaną informację do systemu Pobyt.

Placówka w ramach prowadzonych postępowań administracyjnych w sprawie zobowiązywania cudzoziemców do powrotu, działając w oparciu o przepisy prawa krajowego, tj. art. 324 pkt 1 lub art. 394 ust. 3 ustawy o cudzoziemcach, pobiera odciski linii papilarnych od cudzoziemców powyżej 14 roku życia, zatrzymanych w związku z nielegalnym pobytem na terytorium RP. Cudzoziemiec zatrzymany w związku z nielegalnym pobytem na terytorium RP otrzymuje, w zrozumiałym dla niego języku, pouczenie o zasadach i trybie przeprowadzania kontroli legalności pobytu cudzoziemców na terytorium RP. Dane zawarte w karcie daktyloskopijnej są przesyłane za pośrednictwem systemu informatycznego do CLKP w celu ich zarejestrowania w systemie AFIS. Decyzję o tym, czy pobrane od cudzoziemca dane daktyloskopijne będą sprawdzone i zarejestrowane wyłącznie w systemie AFIS, czy zostaną przesłane również do systemu Eurodac, w każdym przypadku podejmuje placówka. Informacja w powyższym zakresie jest zamieszczana w karcie zawierającej dane personalne cudzoziemca. Numer Eurodac jest nadawany automatycznie przez system informatyczny w trakcie tworzenia karty daktyloskopijnej cudzoziemca za pomocą urządzenia LiveScanner.

W przypadku przyjęcia przez placówkę cudzoziemca przekazanego na podstawie decyzji uwzględniającej wniosek o przejęcie, o którym mowa w rozporządzeniu Dublin III, który złożył następnie wniosek o nadanie statusu uchodźcy, pobierane są w placówce odciski wszystkich palców takiej osoby i przesyłane następnie do CLKP w celu ich zarejestrowania w systemie AFIS oraz w celu ich przekazania do systemu centralnego Eurodac.

Uzyskane informacje o wynikach porównania w systemie Eurodac są wykorzystywane dla celów prowadzonych postępowań administracyjnych w sprawie zobowiązywania cudzoziemców do powrotu w przypadkach i na zasadach określonych w ustawie o cudzoziemcach.

Jak ustalono w toku kontroli przeprowadzonej w UdSC w przypadku uzyskania pozytywnego wyniku weryfikacji w systemie Eurodac, tj. uzyskania trafienia, Straż Graniczna otrzymuje wprowadzony wcześniej przez inne państwo członkowskie numer Eurodac. W przypadku uzyskania trafienia zachodzą przesłanki do wszczęcia przez Szefa UdSC procedury dublińskiej (zgodnie z rozporządzeniem 604/2013). Natomiast w przypadku braku trafienia, gdy cudzoziemiec nie złożył wniosku o ochronę międzynarodową, wszczynana jest przez Straż Graniczną procedura o zobowiązanie do powrotu. W przypadku ubiegania się o udzielenie ochrony międzynarodowej przez cudzoziemca, Straż Graniczna przygotowuje „wniosek o nadanie statusu uchodźcy" oraz przedstawia takiej osobie pouczenia wynikające z rozporządzenia Nr 604/2013, które są sporządzane w zrozumiałym dla niej języku. Straż Graniczna rejestruje wniosek o nadanie statusu uchodźcy w systemie Pobyt i przekazuje papierowy wniosek o nadanie statusu uchodźcy do UdSC. W przypadku ubiegania się o udzielenie ochrony międzynarodowej, wniosek jest wypełniany zawsze, niezależnie od tego, czy nastąpiło trafienie w systemie Eurodac czy też nie. W przypadku nieuzyskania trafienia, jeżeli cudzoziemiec złoży wniosek o udzielenie ochrony międzynarodowej, jest on kierowany do wydziału merytorycznego UdSC. W przypadku trafienia, gdy cudzoziemiec nie złożył wniosku o udzielenie ochrony międzynarodowej w Polsce, Straż Graniczna wnioskuje do Szefa Urzędu o wszczęcie procedury dublińskiej. Procedura dublińska kończy się na ustaleniu państwa odpowiedzialnego za rozpatrzenie wniosku cudzoziemca o udzielenie ochrony międzynarodowej. Po ustaleniu państwa odpowiedzialnego, w zależności od tego, które państwo zostanie uznane za odpowiedzialne za rozpatrzenie wniosku, następuje etap organizowania przekazania cudzoziemca do państwa odpowiedzialnego. W przypadku odpowiedzialności innego państwa członkowskiego procedura o udzielenie ochrony międzynarodowej jest umarzana; w przypadku braku takiego wniosku informowana jest Straż

Graniczna. W przypadku uznania odpowiedzialności Polski akta sprawy są przekazywane do wydziału merytorycznego UdSC celem prowadzenia procedury o udzielenie ochrony międzynarodowej. UdSC nie posiada dostępu do obrazu linii papilarnych przechowywanych w systemie Eurodac. Natomiast w aktach sprawy administracyjnej cudzoziemca znajdują się wydruki kart daktyloskopijnych sporządzone przez Straż Graniczną.

Postępowanie o nadanie statusu uchodźcy kończy się wydaniem przez Szefa UdSC decyzji o nadaniu statusu uchodźcy lub odmowie nadania takiego statusu. W przypadku wydania przez Szefa UdSC decyzji o nadaniu statusu uchodźcy, Szef UdSC, po uprawomocnieniu się decyzji, występuje niezwłocznie na piśmie do CLKP o oznaczenie w systemie Eurodac danych osoby/osób objętej/objętych decyzją. W ramach UdSC prowadzone są również postępowania w sprawie pozbawienia statusu uchodźcy. Postępowania te kończą się wydaniem decyzji przez Szefa UdSC.

Pracownicy UdSC posiadają ograniczony dostęp (do wglądu) za pośrednictwem systemu Pobyt (zakładka o nazwie „Eurodac") do danych zgromadzonych w rejestrze o nazwie „Rejestr cudzoziemców, od których pobrano odciski linii papilarnych". Ww. dostęp jest realizowany wyłącznie w związku z prowadzonymi postępowaniami o nadanie statusu uchodźcy.

Na gruncie powyższych ustaleń, Generalny Inspektor podjął działania mające na celu dokonanie oceny materiału dowodowego zebranego w toku kontroli.

Ponadto w toku kontroli przeprowadzonej w jednej z placówek Straży Granicznej ustalono, że placówka nie występowała do Centralnego Laboratorium Kryminalistycznego Policji z siedzibą w Warszawie o zaktualizowanie zestawu danych dotyczących danej osoby w systemie Eurodac w zakresie dodania informacji o dacie:

1) jej przybycia na terytorium Rzeczypospolitej Polskiej w przypadku przyjęcia przez placówkę cudzoziemca w sytuacji, gdy został on przekazany na podstawie decyzji uwzględniającej wniosek o przejęcie, o którym mowa w rozporządzeniu nr 604/2013,

2) jej przybycia na terytorium Rzeczypospolitej Polskiej – w przypadku przyjęcia przez placówkę cudzoziemca w sytuacji, gdy został on przekazany na podstawie decyzji uwzględniającej wniosek o wtórne przejęcie, o którym mowa w rozporządzeniu nr 604/2013,

3) opuszczenia przez nią terytorium państw członkowskich – w przypadku ustalenia takiej okoliczności przez funkcjonariuszy Placówki,

4) opuszczenia przez nią terytorium państw członkowskich na skutek zrealizowania decyzji organu Straży Granicznej o zobowiązaniu cudzoziemca do powrotu – w przypadku zrealizowania takiej decyzji przez placówkę.

Jak wynika z powyższego, poddana kontroli placówka Straży Granicznej nie realizowała zadań określonych w art. 10 lit. a, lit. b, lit. c i lit. d rozporządzenia nr 603/2013, do wykonywania których zobowiązuje ją również porozumienie zawarte w dniu 1 czerwca 2015 r. pomiędzy Komendantem Głównym Policji, Komendantem Głównym Straży Granicznej, Szefem Urzędu do Spraw Cudzoziemców i Radą do Spraw Uchodźców oraz CLKP dotyczące wzajemnej współpracy oraz koordynacji działań w zakresie realizacji przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 603/2013 w odniesieniu do postępowań administracyjnych prowadzonych w sprawach cudzoziemców[24].

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Komendanta placówki Straży Granicznej o złożenie wyjaśnień w ww. zakresie i przesłanie dowodów potwierdzających usunięcie powyższych uchybień.

W odpowiedzi Komendant placówki poinformował Generalnego Inspektora Ochrony Danych Osobowych, że w placówce trwają obecnie prace nad opracowaniem wewnętrznych procedur celem niezwłocznego rozpoczęcia realizacji zadań określonych w art. 10 lit. a, lit. b, lit. c i lit. d rozporządzenia nr 603/2013. Wskazał również, że przyczyną nierealizowania przez placówkę ww. zadań była błędna interpretacja treści rozporządzenia nr 603/2013 oraz porozumienia zawartego w dniu 1 czerwca 2015 r. pomiędzy Komendantem Głównym Policji, Komendantem Głównym Straży Granicznej, Szefem Urzędu do Spraw Cudzoziemców i Radą do Spraw Uchodźców oraz CLKP, dotyczącego wzajemnej

[24] Stosownie do § 2 pkt 4 porozumienia zawartego w dniu 1 czerwca 2015 r. pomiędzy Komendantem Głównym Policji, Komendantem Głównym Straży Granicznej, Szefem Urzędu do Spraw Cudzoziemców i Radą do Spraw Uchodźców oraz CLKP, *dotyczącego wzajemnej współpracy oraz koordynacji działań w zakresie realizacji przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 603/2013 w odniesieniu do postępowań administracyjnych prowadzonych w sprawach cudzoziemców*, Komendant Główny Straży Granicznej oraz jednostki organizacyjne Straży Granicznej wykonują zadania wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 603/2013 w zakresie występowania do CLKP o zaktualizowanie zestawu danych dotyczących danej osoby w zakresie dodania informacji o dacie: a) jej przybycia na terytorium Rzeczypospolitej Polskiej, w przypadku przekazania na podstawie decyzji uwzględniającej wniosek o przejęcie, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca, zwanym dalej „rozporządzeniem Dublin III", b) jej przybycia na terytorium Rzeczypospolitej Polskiej, w przypadku przekazania na podstawie decyzji uwzględniającej wniosek o wtórne przejęcie, o którym mowa w rozporządzeniu Dublin III, c) opuszczenia przez nią terytorium państw członkowskich, w przypadku ustalenia takiej okoliczności, d) opuszczenia przez nią terytorium państw członkowskich zgodnie z decyzją nakazującą powrót lub w wyniku przymusowego wykonania takiej decyzji.

współpracy oraz koordynacji działań w zakresie realizacji przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 603/2013 w odniesieniu do postępowań administracyjnych prowadzonych w sprawach cudzoziemców w tym zakresie.

2.2.3. Banki i inne instytucje finansowe

W okresie sprawozdawczym w podmiotach należących do sektora banków i innych instytucji finansowych zostało przeprowadzonych **11 kontroli.**

Generalny Inspektor powziął z urzędu informację, iż w jednym z banków[25] w dostępnym systemie bankowości elektronicznej umożliwiającym klientom elektroniczny dostęp do ich rachunków bankowych, historii transakcji, wyciągów, składania w czasie rzeczywistym dyspozycji transakcyjnych, tj. m.in. przelewów krajowych i zagranicznych, dla wszystkich klientów tego banku (niezależnie, czy wnieśli sprzeciw wobec przetwarzania ich danych osobowych w celach marketingowych, czy też nie), w chwili korzystania z systemu bankowości elektronicznej (np. przy dokonywaniu przelewów) wyświetlane są informacje marketingowe.

Wobec powyższego, do tego banku Generalny Inspektor skierował kontrolę w celu ustalenia stanu faktycznego dotyczącego tego typu działań. Ustalenia dokonane w toku kontroli wykazały, iż system bankowości elektronicznej został przed kontrolą zmodyfikowany w taki sposób, iż nie były w nim prezentowane (wyświetlane) informacje marketingowe (reklamy) klientom banku, którzy wnieśli sprzeciw wobec przetwarzania ich danych osobowych w celach marketingowych. Informacje marketingowe w systemie bankowości elektronicznej wyświetlane były wyłącznie w oparciu o wygenerowane z innego systemu informatycznego przez pracowników jednej z komórek organizacyjnych banku pliki zawierające dane osobowe dotyczące wyłącznie klientów, którzy nie wnieśli sprzeciwu wobec przetwarzania ich danych osobowych w celach marketingowych. Kontrola wykazała także, iż w banku opracowane i wdrożone zostały dodatkowe procedury dotyczące prawidłowego i precyzyjnego odnotowywania sprzeciwów wobec przetwarzania danych osobowych wnoszonych przez klientów różnymi kanałami (np. osobiście w placówce banku, w drodze rozmowy telefonicznej, za pomocą poczty elektronicznej). Dokonana zmiana systemu bankowości elektronicznej służącego do wykonywania przez klientów operacji bankowych spowodowała, że w kontrolowanym banku informacje marketingowe (reklamy) prezentowane

[25] Kontrola DIS-K-421/93/15.

(wyświetlane) były jedynie klientom, którzy nie wnieśli sprzeciwu wobec przetwarzania przez bank ich danych osobowych w celach marketingowych. W związku z tym, Generalny Inspektor Ochrony Danych Osobowych nie skorzystał ze swoich ustawowych uprawnień i nie wszczął postępowania administracyjnego w sprawie.

2.2.4. Służba zdrowia

W okresie sprawozdawczym w podmiotach należących do sektora służby zdrowia zostało przeprowadzonych **15 kontroli**.

Spośród wskazanych kontroli 7 dotyczyło przetwarzania[26] danych w elektronicznej dokumentacji medycznej, w systemie informatycznym Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców (eWUŚ) oraz w innych systemach informatycznych, z wyjątkiem sterujących specjalistyczną aparaturą medyczną.

W toku kontroli ustalono, iż kontrolowane podmioty lecznicze przetwarzały dane osobowe pacjentów w postaci tradycyjnej (papierowej) oraz dodatkowo w systemach informatycznych. Systemy informatyczne użytkowane w kontrolowanych podmiotach leczniczych cechowała znaczna różnorodność, wynikająca z tego, iż pochodziły od różnych producentów. Systemy informatyczne były wykorzystywane w ww. podmiotach przede wszystkim do: rejestrowania pacjentów, obsługi skierowań do poradni specjalistycznych, generowania recept, prowadzenia rozliczeń z Narodowym Funduszem Zdrowia (NFZ), przesyłania danych statystycznych dotyczących wykonanych badań, świadczeń. W toku jednej kontroli ustalono również, iż system informatyczny użytkowany był przez podmiot leczniczy także do gromadzenia informacji związanych z przeprowadzanym przez lekarzy w trakcie wizyty lekarskiej wywiadem i badaniem (dane o stanie zdrowia pacjentów).

Podmioty kontrolowane korzystały również z systemów informatycznych Narodowego Funduszu Zdrowia, w szczególności z systemu o nazwie „Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców" („eWUŚ"). Podstawą prawną wprowadzenia systemu Elektronicznej Weryfikacji Uprawnień Świadczeniobiorców jest art. 50 ust. 3 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2015 r. poz. 581 z późn. zm.), zgodnie z którym prawo do świadczeń opieki zdrowotnej może zostać potwierdzone na podstawie dokumentu elektronicznego, o którym mowa w art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności

[26] Np. kontrole DIS-K-421/136/15, DIS-K-421/149/15, DIS-K-421/171/15.

podmiotów realizujących zadania publiczne[27], sporządzonego na podstawie nr PESEL, przez Narodowy Fundusz Zdrowia (NFZ) dla świadczeniodawcy (podmiotu leczniczego) i przesłanego za pomocą środków komunikacji elektronicznej. Podmioty kontrolowane posiadają wydane przez NFZ upoważnienia do korzystania z systemu „eWUŚ", na podstawie przepisów rozporządzenia Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej (Dz. U. z 2012 r. poz. 1500)[28]. Systemy informatyczne w podmiotach kontrolowanych z reguły posiadają funkcjonalność umożliwiającą kierowanie zapytania do systemu „eWUŚ", czy osoby zapisane w danym dniu na wizytę posiadają prawo do świadczeń opieki zdrowotnej, tym samym wyjątkowo sprawdzenia dokonywane były przez pracowników podmiotów leczniczych poprzez stronę internetową NFZ o adresie https://ewus.nfz.gov.pl.

Oceniając wyniki przeprowadzonych kontroli stwierdzić należy, iż podmioty objęte kontrolą zapewniały należyte przetwarzanie danych osobowych pacjentów w systemach informatycznych przez siebie wdrożonych, w szczególności przedmiotowe systemy spełniały warunki określone 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).

Uchybienia stwierdzone w toku kontroli w podmiotach leczniczych polegały na naruszeniu następujących obowiązków wynikających z przepisów o ochronie danych osobowych: niezawarciu pisemnej umowy w przedmiocie przetwarzania danych osobowych

[27] Zgodnie z art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114), dokument elektroniczny to stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.

[28] Stosownie do § 3 ust. 1 rozporządzenia Ministra Zdrowia z dnia 20 grudnia 2012 r. w sprawie warunków występowania o sporządzenie dokumentu elektronicznego potwierdzającego prawo do świadczeń opieki zdrowotnej, w celu uzyskania upoważnienia do korzystania z usługi Elektronicznej Weryfikacji Uprawnień Świadczeniobiorców, świadczeniodawca lub niebędąca świadczeniodawcą osoba uprawniona, składa wniosek o wydanie tego upoważnienia. Zgodnie z ust. 5 ww. przepisu, upoważnienie o którym mowa w ust. 1, zawiera: 1) dane identyfikujące świadczeniodawcę lub niebędącą świadczeniodawcą osobę uprawnioną, o których mowa w ust. 2 pkt 1; 2) zakres upoważnienia, obejmujący uprawnienie świadczeniodawcy lub niebędącej świadczeniodawcą osoby uprawnionej do: a) korzystania z usługi Elektronicznej Weryfikacji Uprawnień Świadczeniobiorców, b) upoważniania osób, którym powierza się wykonywanie zadania w zakresie występowania w jego lub jej imieniu do Funduszu o sporządzenie dokumentu potwierdzającego prawo do świadczeń.

pacjentów (art. 31 ust. 1 ustawy[29]), niespełnieniu przez opracowany dokument odnoszący się do zasad ochrony danych osobowych wymogów przewidzianych dla polityki bezpieczeństwa (§ 4 pkt 2 – 4 rozporządzenia[30]) oraz niezawarciu w ewidencji osób upoważnionych do przetwarzania danych osobowych zakresu upoważnienia do przetwarzania danych (art. 39 ust. 1 pkt 2 ustawy).

Ponadto w toku kontroli stwierdzono w procesie przetwarzania danych osobowych pacjentów nieprawidłowości polegające na: niezastosowaniu środków technicznych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną (art. 36 ust. 1 ustawy[31]), niecelowym pozyskiwaniu zgody na przetwarzanie danych osobowych od pacjentów w sytuacji przetwarzania ich danych na podstawie przepisów prawa, w związku z realizacją umowy, lub w oparciu o prawnie usprawiedliwiony cel administratora danych, tj. marketing własnych produktów i usług (art. 23 ust. 1 ustawy[32]).

Na podstawie wyników kontroli wszczęto postępowania administracyjne w zakresie stwierdzonych uchybień w celu przywrócenia stanu zgodnego z prawem.

Poza opisanymi kontrolami służby zdrowia, do istotnych kontroli podmiotów udzielających świadczeń zdrowotnych należała kontrola przeprowadzona w szpitalu, w związku z informacją przekazaną przez prokuraturę, że doszło do udostępnienia osobom nieupoważnionym zapisanych na płytach CD danych osobowych pacjentów w postaci wyników badań diagnostycznych (RTG)[33]. Płyty te zostały znalezione poza terenem szpitala przez osobę, która powiadomiła o tym organy ścigania. W związku z tym zakresem tej

[29] Art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

[30] Zgodnie z § 4 pkt 2 – 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami.

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

[32] Zgodnie z 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.

[33] Kontrola DIS-K-421/34/15

kontroli objęto zabezpieczenie danych osobowych pacjentów przetwarzanych przez szpital. Analiza zebranego materiału dowodowego wykazała, iż ww. płyty nie były należycie zabezpieczone. Szpital nie zastosował bowiem środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności nie zabezpieczył danych osobowych pacjentów przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Na podstawie wyników kontroli zostało wszczęte postępowanie administracyjne zakończone wydaniem decyzji administracyjnej[34], w której m.in. nakazano usunięcie uchybień w procesie przetwarzania danych osobowych poprzez zabezpieczenie danych osobowych pacjentów. W związku z tym, że szpital nie wykonał decyzji Generalnego Inspektora w tym zakresie, decyzja została przekazana do egzekucji administracyjnej.

2.2.5. Oświata

W toku kontroli przeprowadzonej w jednym z liceum[35] w zakresie przetwarzania danych osobowych uczniów oraz ich rodziców (opiekunów prawnych) stwierdzono, że w szkole zbierane były m.in. takie dane jak nazwa i miejsce pracy rodziców. Tymczasem dopuszczalny zakres danych osobowych uczniów i ich rodziców przetwarzanych przez szkoły został określony w przepisach prawa[36]. W celu prowadzenia przez szkołę dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej za wystarczające uznane zostało przetwarzanie danych osobowych rodziców w zakresie imienia i nazwiska, adresu zamieszkania, adresu poczty elektronicznej i numerów telefonów (taki zakres danych rodziców wynika m.in. z księgi uczniów[37]). Należy zauważyć, że bardziej szczegółowe

[34] Decyzja nr DIS/DEC-616/15/66979

[35] Kontrola DIS-K-421/130/15

[36] Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2004 r. Nr 256, poz. 2572 z późn. zm.) oraz wydane na jej podstawie akty wykonawcze, w tym rozporządzenie Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. z 2014 r. poz. 1170), rozporządzenie Ministra Edukacji Narodowej z dnia 10 czerwca 2015 r. w sprawie szczegółowych warunków i sposobu oceniania i klasyfikowania i promowania uczniów i słuchaczy w szkołach publicznych (Dz. U. z 2015 r., poz. 843), rozporządzenie Ministra Edukacji Narodowej i Sportu z 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach (Dz. U. z 2003 r. Nr 6, poz. 69 z późn. zm.).

[37] § 6 ust. 1 i 2 rozporządzenia Ministra Edukacji Narodowej w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji. Szkoła prowadzi księgę uczniów; do księgi wpisuje się imię (imiona) i nazwisko, datę i miejsce urodzenia, numer PESEL oraz adres zamieszkania ucznia, imiona i nazwiska rodziców

informacje dotyczące rodziców ucznia mogą się pojawiać np. gdy stara się on o pomoc materialną (o której mowa w rozdz. 8a ustawy o systemie oświaty), czy też w sytuacji złożenia oświadczenia o spełnianiu szczególnych kryteriów rekrutacyjnych (art. 20c ust. 2 ustawy o systemie oświaty). Nie dotyczy to jednak wszystkich uczniów, zaś zbieranie takich informacji jest odrębnie uregulowane. W toku kontroli ustalono, że w szkole wprowadzono wzór teczki dla kandydata, będący jednocześnie formularzem zawierającym dane takiej osoby w zakresie: imię, nazwisko, data i miejsce urodzenia, PESEL, imiona i nazwiska rodziców, adres zamieszkania, ucznia i rodziców, miejsce pracy rodziców (nazwa zakładu pracy, adres, telefon), gimnazjum, do którego uczęszczał. W świetle powyższych ustaleń należało stwierdzić, że skoro zakres przetwarzanych przez szkoły danych osobowych został określony w przepisach prawa, to brak jest podstaw prawnych do poszerzania tego katalogu informacji. Odnosząc się do wskazanego w toku kontroli uzasadnienia, iż celem przetwarzania danych dotyczących miejsca pracy rodziców jest zapewnienie bezpieczeństwa dzieciom (np. aby skontaktować się z rodzicem dziecka), należało zauważyć, iż bez pozyskiwania takiej informacji cele te można zrealizować, bowiem rodzic może podać numer telefonu do pracy, numer telefonu służbowego, czy też adres poczty elektronicznej (także ten służbowy). Z tych względów należało uznać, że zbieranie takich danych, jak nazwa i miejsce pracy rodziców było nieuzasadnione w odniesieniu do powołanych przepisów prawa.

2.2.6. Telekomunikacja

W okresie sprawozdawczym u dostawców usług telekomunikacyjnych oraz w podmiotach współpracujących z dostawcami usług telekomunikacyjnych, przeprowadzonych zostało **7 kontroli** zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Zakresem kontroli przeprowadzonej u jednego z dostawców usług telekomunikacyjnych[38] objęto przetwarzanie danych osobowych jego klientów poprzez ustalenie, czy w związku z zawieraniem umów o świadczenie usług telekomunikacyjnych były pozyskiwane kopie dokumentów tożsamości lub innych dokumentów w celu potwierdzenia tożsamości klientów, w tym dowodów osobistych. W toku kontroli ustalono, iż wyrażenie zgody na przetwarzanie przez poddanego kontroli dostawcę usług

oraz adresy ich zamieszkania, jeżeli są różne od adresu zamieszkania ucznia, a także datę rozpoczęcia nauki w danej szkole oraz oddział, do którego ucznia przyjęto.

[38] Kontrola DIS-K-421/51/15

telekomunikacyjnych danych zawartych w skanie przekazywanego dowodu osobistego w celu potwierdzenia tożsamości było niezbędne, aby złożyć zamówienie za pośrednictwem sklepu internetowego. Jeżeli potencjalny klient nie wyraził takiej zgody, to nie zatwierdził złożonego zamówienia i był informowany, iż umowa o świadczenie usług telekomunikacyjnych nie zostanie z nim zawarta poprzez ten kanał sprzedaży. Przetwarzanie przez ww. podmiot danych osobowych pozyskanych ze skanu przekazanego dowodu osobistego, w zakresie szerszym niż wynika to z art. 161 ust. 2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjnego (Dz. U. z 2014 r. poz. 243 z późn. zm.)[39], tj.: koloru oczu, wzrostu, płci, adresu zameldowania, podpisu posiadacza dowodu (w przypadku dowodów osobistych wydawanych przed 1 marca 2015 r.), a także wizerunku twarzy, nazwy organu wydającego dowód osobisty, daty wydania i terminu ważności, naruszało obowiązujące przepisy prawa - art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych[40] - albowiem osobie, której dane dotyczą nie zapewniono swobody w kwestii wyrażenia zgody na ich przetwarzanie (art. 161 ust. 3 ustawy Prawo telekomunikacyjne[41]). Generalny Inspektor wszczął z urzędu postępowanie administracyjne w sprawie wyjaśnienia tej okoliczności. W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego, pełnomocnik Spółki poinformował, iż dostawca usług telekomunikacyjnych dokonał zmiany procedury sprzedaży usług telekomunikacyjnych w kanale sprzedaży internetowej w ten sposób, że nie uzależnia już złożenia zamówienia w sklepie internetowym od wyrażenia zgody na przetwarzanie danych zawartych w skanie dowodu osobistego. Zmieniona procedura nie wymagała od osób zainteresowanych zawarciem umowy o świadczenie usług telekomunikacyjnych w ramach sprzedaży w kanale internetowym, podania danych osobowych w zakresie szerszym niż wskazany w art. 161 ust. 2 Prawa telekomunikacyjnego. Z uwagi na fakt, iż stwierdzone w

[39] Art. 161.2. Dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną: 1) nazwisk i imion; 2) imion rodziców; 3) miejsca i daty urodzenia; 4) adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania; 5) numeru ewidencyjnego PESEL - w przypadku obywatela Rzeczypospolitej Polskiej; 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numeru paszportu lub karty pobytu; 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

[40] Art. 26.1.1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem.

[41] Art. 161.3. Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.

toku kontroli uchybienie w procesie przetwarzania danych osobowych zostało usunięte Generalny Inspektor umorzył postępowanie[42].

W ramach omawianego sektora, w 2015 r. zajęte zostały przez Generalnego Inspektora istotne stanowiska sformułowane na podstawie przeprowadzonych kontroli[43]. Należała do nich kontrola przeprowadzona w jednej ze Spółek[44], w wyniku której ustalono, że do prowadzenia działań marketingowych wobec osób niebędących jej klientami, podmiot ten wykorzystuje m.in. dane osobowe pozyskiwane za pomocą papierowego formularza, który jest dostępny dla osób zainteresowanych w sklepach własnych Spółki. Zakres danych pozyskiwanych za pomocą tego formularza był następujący: imię, nazwisko, numer telefonu, adres poczty elektronicznej, miejscowość. Dane z wypełnionych formularzy były wprowadzane do systemu informatycznego Spółki. Pozyskane w ten sposób dane były wykorzystywane wyłącznie do prowadzenia działań marketingowych, które polegały na podejmowaniu telefonicznego kontaktu z osobą, której dane dotyczą i prezentowaniu jej oferty Spółki, bądź przesyłaniu oferty za pośrednictwem poczty elektronicznej. Podstawą prawną przetwarzania przez Spółkę danych, o których mowa powyżej, jest zgoda na przetwarzanie danych osobowych wyrażona przez osobę, której dane dotyczą (art. 23 ust. 1 pkt 1 ustawy). Ustalono również, że w przypadku odwołania zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, dane jej dotyczące nie były usuwane przez Spółkę. Odwołanie zgody przez osobę, której dane dotyczą, skutkuje natomiast tym, że Spółka ogranicza przetwarzanie danych jej dotyczących wyłącznie do ich przechowywania.

Na podstawie ustalonego w toku kontroli stanu faktycznego oraz w oparciu o obowiązujące przepisy prawa Generalny Inspektor Ochrony Danych Osobowych uznał, że w przypadku wycofania przez osobę, której dane dotyczą, zgody na przetwarzanie danych osobowych, o których mowa powyżej, brak było podstawy prawnej do dalszego ich przetwarzania i dlatego Spółka powinna te dane usunąć. W związku ze stwierdzeniem m.in. powyższego uchybienia w procesie przetwarzania danych osobowych, wobec tego podmiotu zostało wszczęte postępowanie administracyjne zakończone następnie decyzją Generalnego Inspektora Ochrony Danych Osobowych nakazującą Spółce usunięcie uchybień w procesie przetwarzania danych osobowych m.in. poprzez usunięcie danych osobowych pozyskanych

[42] Decyzja DIS/DEC-844/15/93183
[43] Decyzje: DIS/DEC-955/15/105874;DIS/DEC-868/15/96118; DIS/DEC-967/15/106825.
[44] Kontrola DIS-K-421/98/14

za pomocą formularza, a dotyczących osób, które odwołały zgodę na przetwarzanie tych danych przez Spółkę.

Do istotnych należała również kontrola jednego z operatorów telefonii komórkowej[45], przeprowadzona pod koniec 2014 r., ale w związku z którą postępowanie pokontrolne prowadzone było w 2015 r. W jej toku ustalono, że na formularzu umowy o świadczenie usług telekomunikacyjnych podmiot ten pozyskuje od klientów zgodę na przetwarzanie w celach marketingowych spółki lub jej partnerów (tj. innych podmiotów, z którymi spółka współpracuje w zakresie rozpowszechniania informacji handlowej tych podmiotów) danych transmisyjnych związanych z numerami telefonów, z których klient korzysta na podstawie umów zawartych ze Spółką. Zgoda na przetwarzanie danych transmisyjnych w celach marketingowych spółki oraz partnerów została sformułowana jako jedno oświadczenie, które można zaakceptować tylko i wyłącznie akceptując jednocześnie klauzulę zgody na otrzymywanie drogą elektroniczną (np. SMS, MMS, e-mail) informacji handlowych Spółki oraz informacji handlowych jej partnerów oraz klauzulę zgody na używanie automatycznych systemów wywołujących dla celów marketingu bezpośredniego.

Na podstawie ustalonego stanu faktycznego, Generalny Inspektor Ochrony Danych Osobowych uznał, że sposób pozyskiwania przez kontrolowany podmiot zgody na przetwarzanie danych transmisyjnych w celach marketingowych Spółki oraz jej partnerów, nie spełnia wymogu art. 174 pkt 1 ustawy Prawo telekomunikacyjne[46], jako że każda z tych zgód będąc wymuszoną przez konieczność złożenia innych oświadczeń, nie ma charakteru samodzielnego.

W toku kontroli ustalono także, że w przypadku zawierania ze Spółką umowy o świadczenie usług telekomunikacyjnych za pośrednictwem kanału internetowego oraz kanału telefonicznego, warunkiem zawarcia tej umowy było przekazanie Spółce kopii dowodu osobistego dla celów zawarcia i zabezpieczenia tej umowy oraz wyrażenie zgody na przetwarzanie danych osobowych (zawartych w kopii dowodu osobistego) w zakresie: wizerunek, wzrost, kolor oczu oraz adres zameldowania, w celu zawarcia i zabezpieczenia umowy. Wyrażenie zgody, o której mowa powyżej, jest dobrowolne wyłącznie w sytuacji, gdy klient zawiera umowę o świadczenie usług telekomunikacyjnych ze Spółką w sklepie stacjonarnym. W przypadku zawierania umowy o świadczenie usług telekomunikacyjnych za

[45] Kontrola DIS-K-421/138/14

[46] Art. 174. Jeżeli przepisy ustawy wymagają wyrażenia zgody przez abonenta lub użytkownika końcowego, zgoda ta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

pośrednictwem kanału internetowego lub kanału telefonicznego, wyrażenie tej zgody jest obligatoryjne. Dlatego Generalny Inspektor Ochrony Danych Osobowych uznał, że pozyskiwanie przez Spółkę danych osobowych osób zawierających z nią umowę o świadczenie usług telekomunikacyjnych - za pośrednictwem kanału internetowego lub kanału telefonicznego - w zakresie koloru oczu, wzrostu, wizerunku twarzy oraz płci, odbywa się z naruszeniem przepisów prawa.

W związku ze stwierdzonymi uchybieniami w procesie przetwarzania danych osobowych, wobec Spółki zostało wszczęte postępowanie administracyjne, zakończone następnie decyzją Generalnego Inspektora, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych poprzez sformułowanie klauzuli zgody na przetwarzanie przez Spółkę danych transmisyjnych dla celów marketingu jej usług, zamieszczonej w stosowanym przez ten podmiot formularzu umowy o świadczenie usług telekomunikacyjnych, w sposób odrębny od klauzuli zgody na przetwarzanie danych transmisyjnych dla celów marketingu usług podmiotów, z którymi Spółka współpracuje w zakresie rozpowszechniania informacji handlowej tych podmiotów (zwanych dalej również „partnerami Spółki"), przy jednoczesnym zapewnieniu osobom, których dane dotyczą, możliwości odmowy wyrażenia zgody na przetwarzanie danych transmisyjnych dla każdego z ww. celów, a ponadto zapewnieniu, aby wyrażenie tych zgód było niezależne od wyrażenia zgody na otrzymywanie drogą elektroniczną informacji handlowych Spółki i jej partnerów oraz zgody na używanie automatycznych systemów wywołujących dla celów marketingu bezpośredniego, a także poprzez zapewnienie osobom fizycznym zawierającym ze Spółką umowę o świadczenie usług telekomunikacyjnych – za pośrednictwem internetowego oraz telefonicznego kanału sprzedaży – swobody (opcjonalności) w kwestii wyrażenia zgody na przetwarzanie przez Spółkę danych osobowych widniejących w dowodzie osobistym, a wykraczających poza zakres określony w art. 161 ust. 2 ustawy Prawo telekomunikacyjne[47].

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek pełnomocnika Spółki o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 14 kwietnia 2015 r. (DIS/DEC-321/15/29757) oraz o uchylenie zaskarżonej decyzji w zakresie nakazu zawartego w pkt 2 i umorzenie postępowania administracyjnego w tym zakresie. Po dokonaniu ponownej analizy całokształtu materiału dowodowego zebranego w niniejszej sprawie, Generalny Inspektor

[47] Decyzja DIS/DEC-321/15/29757

Ochrony Danych Osobowych, decyzją z dnia 28 lipca 2015 r. (DIS/DEC-622/15/67982), utrzymał w mocy decyzję z dnia 14 kwietnia 2015 r. w zakresie nakazu określonego w pkt 2.

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga Spółki skierowana do Wojewódzkiego Sądu Administracyjnego w Warszawie na decyzję Generalnego Inspektora Ochrony Danych Osobowych z dnia 28 lipca 2015 r. (DIS/DEC-622/15/67982), utrzymującą w mocy decyzję z dnia 14 kwietnia 2015 r. (DIS/DEC-321/15/29757[48]).

2.2.7. Zatrudnienie

W okresie sprawozdawczym, na wniosek Naczelnego Dyrektora Archiwów Państwowych, przeprowadzone zostały kontrole podmiotów przechowujących dokumentację osobową i płacową. W 2015 roku przeprowadzono **14 takich kontroli**[49].

Stan faktyczny ustalony w toku przeprowadzonych czynności kontrolnych był odmienny w każdej kontroli. Stwierdzano przede wszystkim różne okoliczności przejęcia dokumentacji osobowej i płacowej objętej zakresem kontroli: dokumentacja znajdowała się w budynku przejętym przez podmiot kontrolowany; w wyniku zawartej umowy sprzedaży przedsiębiorstwa podmiot kontrolowany nabył od syndyka masy upadłości m.in. dokumentację osobową i płacową; dokumentację przejęto w wyniku następstwa prawnego; porzucona dokumentacja byłej spółdzielni kółek rolniczych została zabezpieczona i była przechowywana przez osobę fizyczną – byłego pracownika ww. podmiotu. Jednocześnie te podmioty, które świadczą usługi w zakresie przechowywania dokumentacji osobowej i płacowej pracodawców, weszły w posiadanie ww. dokumentacji na podstawie zawartych umów przechowania.

Z uwagi na skomplikowany stan faktyczny, a przede wszystkim brak rozwiązań prawnych w opisanym powyżej zakresie, analiza i wykładnia przepisów mogących stanowić podstawę prawną przetwarzania danych osobowych zawartych w przechowywanej dokumentacji osobowej i płacowej była utrudniona. Dodatkowym utrudnieniem odnośnie oceny stanu faktycznego był także znaczny upływ czasu od momentu wejścia w posiadanie przedmiotowej dokumentacji przez podmioty kontrolowane, a także nierzadko kilkukrotne przekształcenia organizacyjno-prawne, jakim podlegały te podmioty na przestrzeni ostatnich

[48] Wyrokiem z dnia 18 lutego 2016 r., sygn. akt II SA/Wa 1655/15, Wojewódzki Sąd Administracyjny oddalił skargę spółki na decyzję Generalnego Inspektora Ochrony Danych Osobowych z dnia 28 lipca 2015 r., nr DIS/DEC-622/15/67982.

[49] Np. kontrole DIS-K-421/56/15, DIS-K-421/75/15, DIS-K-421/78/15 i DIS-K-421/89/15.

lat, co w niektórych przypadkach uniemożliwiło wyczerpujące zebranie materiału dowodowego w prowadzonych przez Generalnego Inspektora postępowaniach.

W toku kontroli ustalono, iż niektórym z podmiotów kontrolowanych przechowujących dokumentację osobową i płacową możliwe było przypisanie przymiotu następcy prawnego podmiotu będącego bezpośrednim wytwórcą ww. dokumentacji. Wskazać także należy, iż niektóre z podmiotów kontrolowanych przechowywały dokumentację osobową i płacową niejako „przy okazji", tj. nie w bezpośrednim związku z prowadzoną przez nich działalnością gospodarczą, a nawet w swoistym „interesie społecznym", mając na uwadze, iż dokumentacja ta będzie potrzebna osobom, których dane dotyczą, do ubiegania się o świadczenie emerytalno-rentowe. (np. w oparciu o zaświadczenia uzyskane od przechowawców).

Problematyka prowadzenia działalności gospodarczej w zakresie przechowywania dokumentacji osobowej i płacowej pracodawców o czasowym okresie przechowywania, a także zasady postępowania z ww. dokumentacją w przypadku likwidacji lub upadłości pracodawcy, zostały unormowane odpowiednio w rozdziałach 4a i 4b ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2015 r. poz. 1446 z późn. zm.)[50]. Z kolei warunki prowadzenia dokumentacji osobowej pracownika określa rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286 z późn. zm.).

Z kolei w przypadku podmiotów objętych zakresem podmiotowym ustawy z dnia 30 sierpnia 1996 r. o komercjalizacji i prywatyzacji (Dz. U. z 2015 r. poz. 747), ww. następstwo

[50] Stosownie do art. 51a ust. 1 ustawy o narodowym zasobie archiwalnym i archiwach, działalność gospodarcza w zakresie przechowywania dokumentacji osobowej i płacowej pracodawców o czasowym okresie przechowywania jest działalnością regulowaną w rozumieniu przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2015 r. poz. 584, z późn. zm.), wykonywaną przez przedsiębiorcę i wymaga uzyskania wpisu do rejestru przechowawców akt osobowych i płacowych. Działalność, o której mowa w ust. 1, może być wykonywana tylko przez przedsiębiorcę będącego osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej (art. 51a ust. 3 powołanej ustawy). Organem prowadzącym rejestr jest marszałek województwa właściwy ze względu na miejsce wykonywania działalności objętej wpisem. Rejestr może być prowadzony w systemie informatycznym (art. 51b ww. ustawy). W myśl art. 51u ust. 1 ustawy o narodowym zasobie archiwalnym i archiwach, w przypadku postawienia pracodawcy w stan likwidacji lub ogłoszenia jego upadłości, odpowiednio likwidator lub syndyk masy upadłości wskazuje podmiot prowadzący działalność w dziedzinie przechowywania dokumentacji, któremu zostanie ona przekazana do dalszego przechowywania, zapewniając na ten cel środki finansowe na czas, jaki pozostał do końca 50-letniego okresu przechowywania dokumentacji liczonego od dnia: 1) zakończenia pracy u danego pracodawcy - dla dokumentacji osobowej; 2) wytworzenia - dla dokumentacji płacowej. W przypadku podmiotów będących spółkami prawa handlowego następstwo prawne wynika z art. 494 § 1 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz. U. z 2013 r. poz. 1030 z późn. zm.). Stosownie do powołanego powyżej przepisu, spółka przejmująca albo spółka nowo zawiązana wstępuje z dniem połączenia we wszystkie prawa i obowiązki spółki przejmowanej albo spółek łączących się przez zawiązanie nowej spółki.

zostało wywiedzione z art. 40 tej ustawy, zgodnie z którym, o ile ustawa nie stanowi inaczej, kupujący lub przejmujący przedsiębiorstwo wstępuje we wszelkie prawa i obowiązki przedsiębiorstwa państwowego, bez względu na charakter stosunku prawnego, z którego te prawa i obowiązki wynikają.

Zaznaczyć należy, iż na skutek przeprowadzonych czynności kontrolnych Generalny Inspektor dostrzegł potrzebę uregulowania stanu prawnego podmiotów, które nie będąc podmiotami objętymi zakresem rozporządzenia Ministra Nauki, Szkolnictwa Wyższego i Techniki z dnia 25 lipca 1984 r. w sprawie zasad klasyfikowania i kwalifikowania dokumentacji oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. z 1984 r. Nr 41, poz. 216), a także następujących po nim aktów prawnych (odnoszących się do organów państwowych, organów jednostek samorządu terytorialnego, państwowych i samorządowych jednostek organizacyjnych) lub podmiotów objętych zakresem art. 51ab ustawy archiwalnej, weszły w posiadanie tej dokumentacji w okresie, gdy brak było regulacji prawnych w tym zakresie i przechowują ją do dnia dzisiejszego, jednakże nie w bezpośrednim związku z prowadzoną działalnością gospodarczą. Uregulowania wymagają także przypadki wejścia w posiadanie dokumentacji osobowej i płacowej - już po wejściu w życie przepisów ustawy archiwalnej - przez podmioty niebędące następcami prawnymi wytwórców tej dokumentacji, które przechowują ją do dnia dzisiejszego, jednakże nie w bezpośrednim związku z prowadzoną działalnością gospodarczą. Ponadto uregulowania wymaga także sytuacja podmiotów, które faktycznie przejmując dokumentację osobową i płacową jako następcy prawni z tytułu przejścia zakładu pracy w trybie art. 231 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2014 r. poz. 1502 z późn. zm.), weszły w posiadanie nie tylko dokumentacji dotyczącej pracowników zatrudnionych w dacie przejścia, lecz także byłych pracowników, wobec których ustał stosunek pracy. Ze względu na opisane problemy z ustaleniem stanu faktycznego, a także brak przepisów prawnych kompleksowo ujmujących problematykę przetwarzania danych osobowych w związku z przechowywaniem dokumentacji osobowej i płacowej, Generalny Inspektor wystąpił do Naczelnego Dyrektora Archiwów Państwowych z wnioskiem o podjęcie działań mających na celu wprowadzenie rozwiązań prawnych, które całościowo uregulują ww. zagadnienia[51].

[51] Pismo z dnia 31 grudnia 2015 r. DIS-108867/15.

Przeprowadzone kontrole wykazały pojedyncze uchybienia w procesie przetwarzania danych osobowych. Stwierdzono w szczególności, iż jeden z podmiotów kontrolowanych świadczy usługi odpłatnego przechowywania dokumentacji osobowej i płacowej bez wymaganego przepisami ustawy archiwalnej wpisu do rejestru przechowawców akt osobowych i płacowych. Inne nieprawidłowości dotyczyły m.in. niezgłoszenia prowadzonego zbioru danych do rejestracji Generalnemu Inspektorowi, niezawarciu wszystkich wymaganych elementów w ewidencji osób upoważnionych do przetwarzania danych osobowych, nieopracowaniu polityki bezpieczeństwa oraz zmienianiu haseł dostępu do systemu informatycznego rzadziej, niż co 30 dni.

W sytuacji, gdzie ustalony w toku kontroli stan faktyczny był jednoznaczny i nie budził wątpliwości (przypadki wykazanego następstwa prawnego, a także usługi świadczone przez podmiot wpisany do rejestru przechowawców) legalność przetwarzania danych osobowych nie budziła wątpliwości. W przypadku czterech podmiotów przechowujących dokumentację osobową i płacową dotyczącą pracowników, dla których pracodawcą nie był podmiot przechowujący, lecz podmioty trzecie, na podstawie wyników kontroli (oraz w niektórych przypadkach po uzupełnieniu materiału dowodowego) prowadzone były postępowania administracyjne w zakresie stwierdzonych uchybień, w celu przywrócenia stanu zgodnego z prawem w procesie przetwarzania danych osobowych.

W stosunku do siedmiu podmiotów, z uwagi na utrudnienia odnośnie braku rozwiązań prawnych oraz problemy dotyczące oceny stanu faktycznego, Generalny Inspektor Ochrony Danych osobowych nie skorzystał z prawa określonego w art. 18 ust. 1 pkt 1 ustawy.

2.2.8. Internet

W toku kontroli Spółki prowadzącej serwis internetowy[52] ustalono, iż podstawą prawną przetwarzania danych osobowych użytkowników w ramach ww. serwisu jest m.in. art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, tj. zgoda osoby, której dane dotyczą. Zgoda wynikała z treści regulaminu serwisu akceptowanej przez użytkownika w momencie rejestracji. W związku z powyższym stwierdzono, iż zastosowana przez spółkę forma pozyskiwania zgody na przetwarzanie danych osobowych naruszała przepisy ustawy o ochronie danych osobowych, bowiem decyzja w sprawie wyrażenia zgody na przetwarzanie danych osobowych nie miała charakteru samodzielnego (zgoda była powiązana z innym oświadczeniem, tj. regulaminem) i swobodnego (postanowienia zawarte w regulaminie uniemożliwiały odmowę wyrażenia zgody

[52] Kontrola DIS-K-421/6/15.

na przetwarzanie danych osobowych). Stanowisko uznające za niezgodne z prawem łączenie oświadczeń woli dotyczących zgody na przetwarzanie danych osobowych znajduje swoje potwierdzenie w orzecznictwie Naczelnego Sądu Administracyjnego. W wyroku z dnia 11 kwietnia 2003 r. (sygn. akt II S.A. 3942/02) Naczelny Sąd Administracyjny stwierdził, iż „(…) w przypadku oświadczenia woli dotyczącego różnych celów przetwarzania (danych osobowych) (…), zgoda winna być wyrażona wyraźnie pod każdym z tych celów przetwarzania". Należy podnieść, iż wyrażający zgodę na przetwarzanie danych osobowych musi mieć pełną świadomość tego, na co się godzi. Spółka zwracając się do użytkownika serwisu o wyrażenie takiej zgody powinna uczynić to w sposób wyraźny, jednoznaczny, wyróżniający się spośród innych pochodzących od Spółki informacji i oświadczeń. W żadnej mierze nie było wystarczające odsyłanie do treści innych dokumentów np. regulaminów czy ogólnych warunków umów (por. wyrok Naczelnego Sądu Administracyjnego z dnia 4 kwietnia 2003 r. sygn. akt II SA 2135/2002). Należało zatem stwierdzić, iż z uwagi na to, że zgoda na przetwarzanie przez spółkę danych osobowych użytkowników serwisu internetowego wynikała z oświadczenia woli o innej treści, tj. regulaminu serwisu internetowego akceptowanego przez użytkownika serwisu w momencie rejestracji, nie był spełniony wymóg określony w art. 7 pkt 5 ustawy o ochronie danych osobowych[53]. Na podstawie wyników kontroli zostało wszczęte postępowanie administracyjne zakończone wydaniem decyzji administracyjnej[54].

Przeprowadzona kontrola innej spółki prowadzącej sklep internetowy[55] wykazała, że do momentu dokonania płatności klient sklepu internetowego miał możliwość anulowania zamówienia. Anulowanie zamówienia nie powodowało jednak usunięcia danych osobowych podanych w związku ze składaniem zamówienia. Z chwilą anulowania zamówienia przez klienta dalsze przetwarzanie danych osobowych zebranych przez spółkę stało się niezgodne z celem, dla którego ww. dane zostały zebrane. W konsekwencji Generalny Inspektor uznał, iż naruszono art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych[56]. Ponadto, w toku kontroli ustalono, że część zamówień na produkty i usługi oferowane w sklepie internetowym składana była przez

[53] Art. 7.5. Ilekroć w ustawie jest mowa o zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

[54] Decyzja nr DIS/DEC-301/15/27031.

[55] Kontrola DIS-K-421/16/15

[56] Art. 26.1.4. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

partnerów (podmioty współpracujące ze spółką w zakresie sprzedaży). Partner dokonując zakupu podawał, jako dane do faktury, dane klienta. Na wystawianych klientom fakturach spółka nie realizowała w całości obowiązku informacyjnego – brak było bowiem informacji o źródle danych oraz o uprawnieniach z art. 32 ust. 1 pkt 7 i 8 ustawy o ochronie danych osobowych[57]. Organ uznał w konsekwencji, iż naruszony został art. 25 ust. 1 pkt 3 i 5 ustawy o ochronie danych osobowych[58]. Ustalono także, iż osoba zakładająca konto po złożeniu zamówienia na wybrane towary lub usługi oferowane w sklepie i podaniu danych kontaktowych, danych do faktury VAT i danych wysyłkowych (o ile nie są tożsame z danymi do faktury VAT) składała jedno oświadczenie w przedmiocie akceptacji regulaminu sklepu i wyrażenia zgody na przetwarzanie danych osobowych na zasadach określonych w tym regulaminie. W ocenie organu naruszało to art. 23 ust. 1 pkt 1[59] w zw. z art. 7 pkt 5 ustawy o ochronie danych osobowych, gdyż zgoda na przetwarzanie danych osobowych stanowiła jedno oświadczenie wraz ze zgodą na akceptację postanowień regulaminu. Ponadto, na stronie głównej spółki znajdował się odnośnik do regulaminu świadczenia usług drogą elektroniczną, którego treść wskazywała, iż odnosi się on również do klientów korzystających ze sklepu internetowego. Regulamin zawierał dwa postanowienia na przetwarzanie danych osobowych usługobiorcy, które zostały zakwestionowane przez organ. Pierwsze odnosiło się do zgody na umieszczenie nazwy (firmy) usługobiorcy na listach klientów spółki. Drugie dotyczyło zgody na przetwarzanie danych osobowych podanych przy rejestracji na potrzeby kilku celów spółki i podmiotów z nią współpracujących (m.in. udostępnianie, promocja i reklama obcych towarów i usług). Generalny Inspektor uznał, iż ww. zgody zostały skonstruowane w sposób wadliwy – usługobiorca nie miał możliwości swobodnego wyrażenia zgody. Obydwie były częścią ww. dokumentu, zaś regulamin zawierał także uregulowanie zobowiązujące usługobiorcę do przestrzegania wszystkich jego postanowień. Oznaczało to, iż ww. zgody były domniemane z oświadczenia woli o innej treści, bowiem spółka przyjęła, iż każdy usługobiorca akceptując regulamin tym samym wyraża zgodę na przetwarzanie jego danych osobowych do wskazanych powyżej celów.

[57] Art. 32.1.7 i 8. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację oraz do wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

[58] Art. 25.1.3 i 5. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o źródle danych i o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

[59] Art. 23.1.1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych.

Cel przetwarzania polegający na umieszczeniu nazwy (firmy) usługobiorcy na listach klientów spółki oznaczał w istocie ich udostępnienie. Udostępnienie to następowało w związku z działaniem o charakterze marketingowym. Stanowiło ono odrębny od przetwarzania danych osobowych na potrzeby realizacji umowy cel przetwarzania. W tym zakresie doszło zatem również do naruszenia art. 23 ust. 1 pkt 1 w zw. z art. 7 pkt 5 ustawy o ochronie danych osobowych, gdyż zgoda na przetwarzanie danych osobowych była domniemana z oświadczenia woli o innej treści, zaś użytkownik pozbawiony był możliwości swobodnego wyrażenia woli w przedmiocie tej zgody. Odnośnie drugiego z postanowień organ uznał także, iż nie umożliwia ono swobodnego wyrażenia woli w przedmiocie zgody na przetwarzanie danych do każdego z celów przetwarzania.

W związku ze stwierdzonymi uchybieniami Generalny Inspektor wszczął postępowanie administracyjne w sprawie. W jego toku spółka usunęła część z zarzucanych uchybień. Postępowanie zakończyło się wydaniem decyzji[60] nakazującej spółce zaprzestanie przetwarzania danych osobowych klientów sklepu internetowego w związku ze złożonym przez nich zamówieniem, które następnie zostało anulowane przez klienta, a także usunięcie dotychczas zebranych danych osobowych klientów sklepu internetowego w związku ze złożonym przez nich zamówieniem, które następnie zostało anulowane przez klienta. W pozostałym zakresie organ umorzył postępowanie.

2.2.9. Wypożyczalnie sprzętu sportowego i audioprzewodników

W 2015 r. przeprowadzono **12 kontroli w podmiotach zajmujących się wypożyczaniem sprzętu sportowego i audioprzewodników,** w tym w 11 prowadzących wypożyczalnie sprzętu sportowego[61] i w 1 wypożyczającym audioprzewodniki[62].

W poddanych kontroli podmiotach stwierdzono przypadki zatrzymywania „w zastaw" dokumentów zawierających dane osobowe osób wypożyczających sprzęt. W kilku podmiotach sprzęt był wypożyczany za pozostawieniem przez wypożyczającego kaucji. W przypadku wypożyczenia za kaucją, klient otrzymywał potwierdzenie w formie blankietu z kolejnym numerem. Jeżeli wypożyczający nie zdecydował się na wypożyczenie sprzętu za kaucją, mógł wypożyczyć sprzęt za dobrowolnym pozostawieniem ważnego dokumentu ze zdjęciem, na zasadach określonych w obowiązującym regulaminie, który nie precyzował,

[60] Decyzja nr DIS/DEC-593/15/62551.
[61] Np. kontrole DIS-K-421/12/15, DIS-K-421/19/15, DIS-K-421/23/15 i DIS-K-421/28/15.
[62] Kontrola DIS-K-421/46/15

jakiego rodzaju ma to być dokument, pozostawiając to decyzji wypożyczającego (w sporadycznych przypadkach był to dowód osobisty). Zazwyczaj pozostawianymi dokumentami były: prawo jazdy, legitymacja szkolna lub studencka, karta miejska. Wypożyczającemu w chwili oddania wypożyczonego sprzętu, zwracany był pozostawiony przez niego dokument. W toku oględzin przeprowadzonych podczas kontroli stwierdzono, iż w wypożyczalniach przechowywano prawa jazdy, legitymacje studenckie, patent żeglarski i karty miejskie.

Dokonana w związku z ww. ustaleniami analiza obowiązujących przepisów prawa wykazała brak podstaw prawnych do zatrzymywania dowodów osobistych i innych dokumentów, a także gromadzenia danych osobowych zawartych w okazanych dokumentach w zakresie szerszym, niż jest to niezbędne w stosunku do celu zbierania danych. Zgodnie z art. 4 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. poz. 167, poz. 1131 z późn. zm.), dowód osobisty jest dokumentem stwierdzającym tożsamość i obywatelstwo polskie osoby na terytorium Rzeczypospolitej Polskiej oraz innych państw członkowskich Unii Europejskiej, państw Europejskiego Obszaru Gospodarczego nienależących do Unii Europejskiej oraz państw niebędących stronami umowy o Europejskim Obszarze Gospodarczym, których obywatele mogą korzystać ze swobody przepływu osób na podstawie umów zawartych przez te państwa ze Wspólnotą Europejską i jej państwami członkowskimi oraz na podstawie jednostronnych decyzji innych państw, uznających ten dokument za wystarczający do przekraczania ich granic. Dowód osobisty uprawnia do przekraczania granic państw, o których mowa w ust. 1. Wskazana ustawa nakłada na każdego pełnoletniego obywatela Rzeczypospolitej Polskiej zamieszkującego na jej terytorium, obowiązek posiadania dowodu osobistego (art. 5 ust. 2 ww. ustawy).

Stosownie zaś do art. 79 pkt 2 ustawy o dowodach osobistych, zatrzymywanie bez podstawy prawnej cudzego dowodu osobistego jest zagrożone karą ograniczenia wolności albo karą grzywny. Zatrzymywanie dowodów osobistych przez przedsiębiorców lub inne podmioty w związku z wypożyczaniem sprzętu nie znajduje podstaw w jakichkolwiek regulacjach prawnych, a zatem stanowi działanie bezprawne. Każdy, kto nie będąc do tego uprawnionym na podstawie odrębnych, powszechnie obowiązujących przepisów prawa, stosuje tego typu praktyki, naraża się na odpowiedzialność za wykroczenie. Z wykroczeniem mamy do czynienia w przypadkach wymuszenia pozostawienia dowodu wskutek uzależnienia dokonania określonej usługi od zatrzymania dowodu osobistego przez wykonującego usługę. Sąd Apelacyjny w Katowicach w wyroku z dnia 9 grudnia 2010 r. (sygn. II Aka 397/10)

wskazał, iż „znamię czasownikowe „zatrzymanie" należy rozumieć jako pozbawienie władztwa, odebranie, a więc chodzi o zachowanie sprzeczne z wolą dysponenta dowodu osobistego. Zatem jedynie zatrzymanie dowodu osobistego wbrew woli i akceptacji jego właściciela może prowadzić do wyczerpania znamion wykroczenia określonego w art. 55 ust. 1 pkt 2 ustawy o ewidencji ludności i dowodach osobistych". Trudno jednak mówić o zgodzie właściciela, dowolności i przyzwoleniu na zatrzymanie dowodu osobistego w sytuacji, kiedy wykonanie danej usługi zostało uzależnione od oddania dowodu osobistego na czas jej wykonywania. Żądanie pozostawienia dowodu osobistego na polecenie i do dyspozycji podmiotu, który uzależnia wykonanie przez niego usługi od czasowego pozostawienia dowodu osobistego, nie ma nic wspólnego z akceptacją i odbywa się wbrew woli i bez przyzwolenia właściciela.

Ponadto należy podkreślić, iż zatrzymywanie jakichkolwiek innych dokumentów, których posługiwanie się służy konkretnym celom określonym przez przepisy prawa, niezgodnie z tymi celami, również jest niedopuszczalne. Praktyka zatrzymywania w innych niż wskazane przez prawo celach dokumentów należących do osób wypożyczających sprzęt lub inne urządzenia, takich jak: paszport, prawo jazdy, dowód rejestracyjny pojazdu, legitymacja szkolna, legitymacja studencka, legitymacja emeryta – rencisty, książeczka wojskowa, nie jest zatem w żaden sposób uprawniona. Do zatrzymania np. prawa jazdy lub dowodu rejestracyjnego pojazdu uprawnione są jedynie podmioty wymienione w przepisach prawa, do których należy m.in. Policja, i to tylko w ściśle w określonych sytuacjach. Należy również podnieść, jak wskazał NSA w wyroku z dnia 16 lutego 2007 r., że „Prawo jazdy jest wyłącznie dokumentem stwierdzającym uprawnienie do kierowania pojazdem silnikowym, nie zaś dokumentem potwierdzającym tożsamość, dlatego informacje w zakresie kategorii i daty nadania uprawnienia do prowadzenia pojazdów są zbędne dla realizacji celu ich zbierania tj. identyfikacji osoby." (I OSK 478/06), nie ma zatem podstaw do wykorzystywania tego dokumentu dla celów innych niż potwierdzenie posiadanych uprawnień.

Podkreślenia również wymaga, iż dokumenty nie mogą stanowić przedmiotu zastawu, a tym samym nie mogą być w tym celu zatrzymywane. Takie stanowisko znajduje potwierdzenie w uchwale Sądu Najwyższego z dnia 18 września 1972 r. (sygn. III CZP 59/72), z którego wynika, że *„papiery i dokumenty (...) nie mają samoistnej wartości. Stwierdzają one jedynie istnienie określonego prawa. Dlatego też nie mogą być przedmiotem zastawu na rzeczach ruchomych.*"

Jednocześnie istotne jest wskazanie, iż zgodnie z art. 23 ust. 1 ustawy o ochronie danych osobowych, aby wykorzystywanie danych osobowych zawartych w dokumentach mogło być uznane za legalne, musi odbywać się w oparciu o wskazaną w przepisach podstawę prawną i w zakresie adekwatnym do celu przetwarzania tych danych (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych[63]). Niewątpliwie przesłankę przetwarzania danych osobowych przez wypożyczających sprzęt (urządzenie) wskazaną w art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych, stanowi konieczność 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. Celem pozyskania danych w sytuacji zawarcia umowy wypożyczenia sprzętu lub urządzenia może być przede wszystkim realizacja ewentualnych roszczeń wynikających z tej umowy, tj. wniesienia pozwu w przypadku kradzieży wypożyczonego sprzętu/urządzenia lub jego zniszczenia. Tymczasem dokumenty takie jak wskazane powyżej, zawierają większy zakres danych osobowych, niż to jest konieczne dla zawarcia i realizacji umowy. We wskazanym celu zasadne jest zatem spisanie (zeskanowanie) tylko niezbędnych danych. Jeśli zatem celem zbierania danych na podstawie dokumentów potwierdzających tożsamość ma być dochodzenie roszczeń, to wystarczy pozyskanie tylko takich danych identyfikujących osobę, jak np. imię, nazwisko, adres zamieszkania i ewentualnie numer PESEL. Jednocześnie należy podkreślić, iż równie skuteczny dla obu stron umowy wydaje się środek w postaci kaucji za wypożyczenie, niepowodujący konieczności pozyskiwania danych osobowych, a jednocześnie zabezpieczający ewentualne roszczenia usługodawców wypożyczających takie urządzenia. Z powyższych względów uznano, że podmioty, które zatrzymywały ww. dokumenty, zbierały dane w zakresie szerszym, niż jest to niezbędne dla zabezpieczenia ich ewentualnych roszczeń.

Wątpliwości wzbudziły również treści stosowanych przez wypożyczalnie regulaminów, których postanowienia nie odpowiadały stanowi faktycznemu i prawnemu stwierdzonemu w toku przeprowadzonych w tych podmiotach kontroli, np. w odniesieniu do zakresu zbieranych danych. Ponadto wskazywały, że przesłanką przetwarzania danych jest zgoda wyrażana poprzez akceptację regulaminu. Tymczasem, jak wskazano, podstawę stanowi realizacja umowy, której stroną jest wypożyczający.

[63] Art.26.1.3. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

Oprócz ww. uchybienia kontrole podmiotów wypożyczających sprzęt sportowy i audioprzewodniki wykazały również inne nieprawidłowości w procesie przetwarzania danych osobowych, tj. w szczególności niedopełnienie w całości lub w części obowiązku informacyjnego, nieopracownie dokumentacji stanowiącej politykę bezpieczeństwa lub nieuwzględnienie w niej wszystkich wymaganych elementów oraz nienadanie upoważnień osobom dopuszczonym do przetwarzania danych.

Z uwagi na to, iż większość skontrolowanych podmiotów działała sezonowo i w trakcie prowadzenia czynności pokontrolnych przestała prowadzić wypożyczalnie, a tym samym zakończyła też przetwarzanie danych w związku z tą działalnością, brak było podstaw do zastosowania środków, o których mowa w art. 18 ust. 1 ustawy o ochronie danych osobowych[64]. Podmioty te zostały poinformowane o stwierdzonych nieprawidłowościach i konieczności ich usunięcia w przypadku prowadzenia wypożyczalni w kolejnych sezonach. Wobec jednego z podmiotów, który prowadzi całorocznie wypożyczalnię sprzętu, wszczęte zostało postępowanie administracyjne i wydana została decyzja nakazująca usunięcie uchybień[65].

2.2.10. Pozostałe kontrole

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

W toku jednej z kontroli[66] ustalono, że skontrolowany podmiot (Spółka) przetwarza nr PESEL w celu ewidencji osób wchodzących do budynków Spółki oraz z nich wychodzących. W ocenie Generalnego Inspektora pozyskiwanie nr PESEL od osób wchodzących do budynku nie było niezbędne do osiągnięcia celu przetwarzania danych osobowych. Mając na względzie, że na podstawie nr PESEL oprócz potwierdzenia tożsamości osoby, której numer ten jest przyporządkowany, można również ustalić m.in. datę urodzenia tej osoby i płeć, należało uznać, iż zakres danych pozyskiwanych przez ten podmiot był zbyt szeroki i nieadekwatny do celu przetwarzania tych danych. Za nienaruszające zasady adekwatności

[64] 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.

[65] Decyzja DIS/DEC-681/15/76325.

[66] Kontrola DIS-K-421/15/15

orzecznictwo sądowe uznaje odnotowywanie tylko imienia, nazwiska i numeru dokumentu służącego do identyfikacji osób w celu zapewnienia bezpieczeństwa budynku (por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 12 maja 2005 r. sygn. II SA/Wa 2499/00, niepublikowane). W związku z powyższym należało uznać, iż stosowana przez ten podmiot praktyka polegająca na przetwarzaniu nr PESEL osób wchodzących do budynków była niezgodna z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. Wobec powyższego, wobec spółki zostało wszczęte postępowanie administracyjne zakończone wydaniem decyzji administracyjnej[67]. Spółka wykonała nakaz decyzji w zakresie zaprzestania przetwarzania numerów PESEL w celu ewidencji osób wchodzących do budynków spółki oraz z nich wychodzących.

Do istotnych należała również kontrola Spółki prowadzącej obiekt sportowy, na terenie którego znajduje się kompleks basenów, obejmującej swym zakresem dane utrwalone przy użyciu elektronicznych urządzeń rejestrujących obraz (monitoring zewnętrzny i wewnętrzny budynku)[68]. W toku kontroli ustalono, iż kontrolowany podmiot przetwarza dane osobowe osób uprawnionych do przebywania na terenie obiektu w postaci wizerunków tych osób w systemie telewizji przemysłowej (monitoring wizyjny) rejestrującym wizerunki osób oraz obraz zarówno terenu zewnętrznego, jak i wewnętrznego tego obiektu. Ustalenia wykazały, iż system telewizji przemysłowej nie rejestruje głosu ww. osób. Monitoring wizyjny zainstalowany został na terenie kompleksu w celu zapewnienia bezpieczeństwa jego klientom oraz mieniu poprzez kontrolę dostępu do pomieszczeń zgodnie z uprawnieniami nadanymi przez Spółkę dla każdej osoby przebywającej na terenie tego kompleksu oraz zapobiegania wszelkiego rodzaju incydentom (kradzieże, picie alkoholu, itp.). System monitoruje następujący obszar: baseny sportowe wewnętrzne (kamery skierowane na niecki basenowe i otoczenie oraz na ciągi komunikacyjne, w tym na ciągi komunikacyjne w szatniach), baseny rekreacyjne wewnętrzne (kamery skierowane na niecki basenowe i otoczenie, na ciągi komunikacyjne, w tym na ciągi komunikacyjne w szatniach) oraz baseny zewnętrzne wraz z plażami zewnętrznymi, parkingiem i odwiertem (kamery skierowane na niecki basenowe, parking i odwiert wody). Urządzenia monitorujące nie zostały zainstalowane w miejscach, w których naruszałyby dobra osobiste osób odwiedzających kompleks, tj. w toaletach, salach prysznicowych, przebieralniach i saunach. Ustalenia dokonane w toku kontroli wykazały, iż kamery umieszczone we wszystkich szatniach znajdujących się w kompleksie skierowane są

[67] Decyzja nr DIS/DEC-441/15/41273
[68] Kontrola DIS-K-421/159/15

na ciągi komunikacyjne szatni. W wyniku oględzin stanowiska monitoringu stwierdzono, iż zapisany w systemie informatycznym obraz pochodzący z kamer zamieszczonych w ww. szatniach, wyświetlany na monitorach tego systemu, rejestrował obraz z ciągów komunikacyjnych szatni, natomiast nie rejestrował obrazu z przebieralni umieszczonych przy tych szatniach. Oględziny pomieszczeń wykazały także, iż przed wejściem do każdej szatni kompleksu zamieszczona była informacja o tym, że pomieszczenie szatni jest monitorowane w sposób ciągły w celu zapewnienia bezpieczeństwa jego klientom oraz mieniu zarówno przez nich wniesionemu na teren kompleksu, jak i mieniu Spółki. Zamieszczona była także informacja o nazwie i adresie siedziby administratora danych osobowych przetwarzanych w systemie telewizji przemysłowej. Na podstawie ustalonego stanu faktycznego, Generalny Inspektor uznał, że Spółka w zakresie objętym kontrolą nie narusza przepisów o ochronie danych osobowych. W związku z tym Generalny Inspektor nie skorzystał z prawa określonego w art. 18 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

Kolejna opisywana kontrola przeprowadzona została w Spółce prowadzącej program, w ramach którego oferowała swoim klientom (będącym pracodawcami) możliwość skorzystania przez ich pracowników oraz osoby wskazane przez tych pracowników (osoby towarzyszące i dzieci) z programu dostępu do obiektów sportowych partnerów Spółki na podstawie stosownych kart[69]. W toku kontroli ustalono, że klienci zawierali ze Spółką umowę o świadczenie usług, której przedmiotem było świadczenie usług na rzecz posiadaczy kart przez Spółkę i jej partnerów. W większości przypadków w treści umowy klienci powierzali Spółce, zgodnie z art. 31 ust. 1 ustawy o ochronie danych osobowych[70], przetwarzanie danych osobowych posiadaczy kart, zaś w niektórych przypadkach Spółka powierzała przetwarzanie danych osobowych posiadaczy kart klientom i wówczas pozyskiwała od tych osób zgodę na przetwarzanie danych ich dotyczących. Istotą programu było to, że posiadacze kart w pełni dobrowolnie decydowali o sposobie korzystania z produktów i usług oferowanych przez Spółkę w ramach tego programu. To pracownicy klientów Spółki decydowali, czy chcą przystąpić do tego programu oraz czy chcą, aby inne osoby (określone jako osoby towarzyszące i dzieci) również korzystały z tych produktów i usług. Pracodawca nie mógł udostępnić Spółce danych tych osób bez ich wiedzy i zgody.

[69] Kontrole DIS-K-421/135/14 i DIS-K-421/11/15.

[70] Art. 31.1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

Z definicji administratora danych, określonej w art. 7 pkt 4 ustawy o ochronie danych osobowych[71], wynika, iż decydując o celach i środkach przetwarzania danych, w przypadku ich powierzenia, nie może być on ograniczony zgodą osoby, której dane dotyczą. Tym samym uznać należało, że klient nie mógł powierzyć Spółce przetwarzania danych posiadaczy kart w ramach umowy powierzenia, o której mowa w art. 31 ustawy o ochronie danych osobowych, gdyż przetwarzanie tych danych było uzależnione właśnie od zgody osób, których one dotyczą. Instytucja powierzenia przetwarzania danych osobowych podmiotowi trzeciemu polega m.in. na tym, iż nie jest wymagane uzyskanie zgody osoby, której dane dotyczą, na powierzenie jej danych. Powierzenie przetwarzania danych osobowych nie wymaga również informowania osób zainteresowanych o takiej czynności, zgodnie z art. 24 ust. 1 pkt 2 ustawy o ochronie danych osobowych[72] lub art. 25 ust. 1 pkt 2 ustawy o ochronie danych osobowych[73]. Zgodnie bowiem z art. 7 pkt 6 ustawy o ochronie danych osobowych[74] podmiot, któremu powierzono przetwarzanie danych osobowych, nie jest traktowany jako odrębny „odbiorca" danych. A zatem z uwagi na to, iż klient jedynie za wiedzą i zgodą mógł udostępnić Spółce dane pracowników, osób towarzyszących i dzieci, nie mogło się to odbywać w drodze umowy powierzenia Spółce przetwarzania danych przez klienta, o której mowa w art. 31 ustawy o ochronie danych osobowych. Pracodawca przetwarza dane osobowe pracowników w zakresie i celu niezbędnym dla wykonania ciążących na nim obowiązków wynikających ze stosunku pracy. A zatem, jako administrator danych, może jedynie w tym celu powierzyć innemu podmiotowi przetwarzanie tych danych. Umożliwienie natomiast

[71] Art. 7.4. Ilekroć w ustawie jest mowa o administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych

[72] Art. 24.1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku; celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych; prawie dostępu do treści swoich danych oraz ich poprawiania; dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

[73] Art. 25.1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku; celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych; źródle danych; prawie dostępu do treści swoich danych oraz ich poprawiania; uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy.

[74] Art. 7.6. Ilekroć w ustawie jest mowa o: odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osoby upoważnionej do przetwarzania danych; przedstawiciela, o którym mowa w art. 31a; podmiotu, o którym mowa w art. 31; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

pracownikowi uczestnictwa w zajęciach sportowych w ramach programu nie należy do takich obowiązków.

Jednocześnie na podstawie materiału dowodowego należało stwierdzić, iż to Spółka decydowała o celach i środkach przetwarzania danych posiadaczy kart. Klient co prawda posiadał swobodę wyboru, czy karty będą imienne czy też na okaziciela, jednakże w przypadku, gdy zdecydował się na karty imienne, to Spółka określała, jaki zakres danych osobowych był niezbędny dla wystawienia takich kart. Jeżeli klient natomiast zdecydował się na karty na okaziciela, nie dochodziło do przetwarzania danych osobowych przez Spółkę. Ponadto z materiału dowodowego wynikało jednoznacznie, iż brak było uzasadnienia, aby klient (pracodawca) pozyskiwał od tego podmiotu informacje, w jaki sposób zgłoszeni przez niego posiadacze kart korzystali z usług oferowanych w ramach programu. W przypadku bowiem kart imiennych opłatę za korzystanie z programu w określonej w umowie wysokości uiszczał klient, albo klient wspólnie z posiadaczem karty lub sam posiadacz karty. Stosownie do postanowień umowy o świadczenie usług zawieranej przez Spółkę z klientami, koszt dostępu ponoszony przez klienta lub posiadacza karty na rzecz Spółki był określony kwotą wskazaną w tej umowie. Koszty te były niezależne od sposobu (ilości wizyt posiadaczy kart w obiektach sportowych), w jaki uczestnicy korzystali z obiektów sportowych w ramach tego programu. Jak wynika z powyższego, dane o sposobie korzystania z programu w żaden sposób nie wpływały na warunki finansowe umów zawartych przez klientów ze Spółką. Rola klienta sprowadzała się do poinformowania Spółki, jakie osoby wyraziły wolę uczestnictwa w programie oraz ponoszenia lub nie części lub całości kosztów udziału tych osób w programie. Spółka natomiast płaciła partnerom, do których należały obiekty sportowe objęte programem, kwotę zależną od ilości wizyt posiadaczy kart. Tym samym w interesie Spółki (a nie klientów) było, aby z karty imiennej korzystali wyłącznie ich posiadacze, ponieważ korzystanie z tej karty przez inne osoby niż jej posiadacz podnosiłoby koszt jej użytkowania ponoszony przez Spółkę na rzecz jej partnerów, a jak wskazano wyżej, opłata za korzystanie z karty ponoszona przez klienta lub posiadacza karty była stała, niezależna od powyższych okoliczności. Wynikało to też wprost z treści regulaminu, stanowiącego załącznik do umowy o świadczenie usług w ramach programu. Zgodnie z postanowieniami regulaminu karta przypisana danej osobie (karta imienna) nie mogła być udostępniana innym osobom. Przedstawiciel Spółki (kontroler) lub pracownik partnera byli upoważnieni do weryfikacji karty z dokumentem tożsamości oraz do zatrzymania karty użytkowanej niezgodnie z jej przeznaczeniem lub postanowieniami regulaminu. Niezbędna była zatem

weryfikacja przez partnerów Spółki tożsamości posiadaczy kart zamierzających skorzystać z ich usług w ramach programu, co było równoznaczne z przetwarzaniem danych tych osób w celu określonym przez Spółkę, to jest zapewnieniem, aby z karty korzystał wyłącznie jej posiadacz.

Wobec powyższego, Generalny Inspektor stanął na stanowisku, iż to Spółka była administratorem danych posiadaczy kart. Z uwagi natomiast na to, iż tylko niektórzy z posiadaczy kart wyrażali zgodę na przetwarzanie ich danych osobowych przez ten podmiot, jako administratora tych danych, uznać należało, iż w przypadku pozostałych posiadaczy kart, którzy takiej zgody nie udzielili, Spółka nie legitymowała się przesłanką, o której mowa w art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych, uprawniającą do przetwarzania ich danych osobowych.

W związku ze stwierdzonym uchybieniem w procesie przetwarzania danych osobowych, o którym mowa powyżej, zostało wszczęte postępowanie administracyjne. Generalny Inspektor Ochrony Danych Osobowych nakazał w drodze decyzji administracyjnej jego usunięcie[75].

W toku innej z kontroli[76] ustalono, iż w związku z prowadzoną działalnością Spółka utworzyła zbiór obejmujący dane osób, które wzięły udział w ankietach i konkursach organizowanych przez ten podmiot. Zakres danych przetwarzanych w ww. zbiorze obejmował imię, nazwisko, datę urodzenia, adres zamieszkania, nr telefonu, adres e-mail, adres IP komputera oraz preferencje konsumpcyjne. Dane były przetwarzane w celach promocyjnych, reklamowych i marketingowych Spółki i podmiotów trzecich oraz były udostępniane w tych celach podmiotom trzecim. Podstawą prawną przetwarzania danych ww. osób była zgoda osoby, której dane dotyczą. Ww. zgoda była wyrażana na formularzach zamieszczonych na poszczególnych stronach internetowych Spółki. W toku analizy treści zgód ustalono, iż brak było swobody w wyrażeniu zgody na przetwarzanie danych osobowych w celach marketingowych podmiotów trzecich oraz zgody na udostępnianie danych podmiotom trzecim, które będą je przetwarzały w celach marketingowych w ramach prowadzonych konkursów i ankiet.

Mając powyższe na uwadze wskazano, że zgoda na przetwarzanie danych osobowych w celach marketingowych produktów i usług podmiotów trzecich nie może stanowić jednocześnie zgody na udostępnianie danych innym podmiotom. Wskazano także, że

[75] Decyzja DIS/DEC-594/15/62961
[76] Kontrola DIS-K-421/114/15

niedopuszczalne jest zawieranie klauzul zgody na przetwarzanie danych osobowych w treści regulaminów, gdzie osoba podająca swoje dane nie ma możliwości swobodnego złożenia oświadczenia w przedmiocie przetwarzania jej danych.

Ponadto kontrola wykazała, iż na formularzach internetowych zamieszczonych na stronach internetowych konkursów i ankiet znajdowały się klauzule zgody dotyczące przetwarzania danych na podstawie przepisów ustawy o świadczeniu usług drogą elektroniczną i ustawy prawo telekomunikacyjne. Z analizy treści ww. zgód ustalono, iż dane pozyskiwane na ich podstawie były przetwarzane niezgodnie z prawem, tj. art. 4 i 10 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 z późn. zm.)[77] oraz art. 172 ust. 1 i 2 oraz art. 174 ustawy Prawo telekomunikacyjne[78], tj. poprzez brak swobody w wyrażeniu zgody na otrzymywanie informacji handlowych drogą elektroniczną zgodnie z ustawą o świadczeniu usług drogą elektroniczną oraz zgody na otrzymywanie informacji marketingowych poprzez użycie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących na podstawie ustawy prawo telekomunikacyjne.

Mając powyższe ustalenia na uwadze wskazano, że w przypadku pozyskiwania przez Spółkę od osób, które biorą udział w konkursie lub ankiecie, w jednej klauzuli zgody na otrzymywanie informacji handlowych drogą elektroniczną zgodnie z ustawą o świadczeniu usług drogą elektroniczną oraz zgody na otrzymywanie informacji marketingowych poprzez użycie automatycznych systemów wywołujących na podstawie ustawy prawo telekomunikacyjne, stanowiło naruszenie przepisów art. 4 ustawy o świadczeniu usług drogą elektroniczną oraz art. 174 ustawy prawo telekomunikacyjne, gdyż ww. zgody powinny być odrębne, aby zadośćuczynić ww. przepisom, tj. zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgody te muszą być sformułowane w sposób

[77] Art. 4.1. Jeżeli ustawa wymaga uzyskania zgody usługobiorcy, to zgoda ta: 1) nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; 2) może być odwołana w każdym czasie. 2. Usługodawca wykazuje uzyskanie zgody, o której mowa w ust. 1, dla celów dowodowych. Art. 10.1. Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. 2. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny. 3. Działanie, o którym mowa w ust. 1, stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy, o której mowa w art. 9 ust. 3 pkt 1.

[78] Art. 172. 1. Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę. 2. Przepis ust. 1 nie narusza zakazów i ograniczeń dotyczących przesyłania niezamówionej informacji handlowej wynikających z odrębnych ustaw. Art. 174. Jeżeli przepisy ustawy wymagają wyrażenia zgody przez abonenta lub użytkownika końcowego, zgoda ta: 1) nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; 2) może być wyrażona drogą elektroniczną, pod warunkiem jej utrwalenia i potwierdzenia przez użytkownika; 3) może być wycofana w każdym czasie, w sposób prosty i wolny od opłat.

wyraźny i jednoznaczny i wyróżniać się spośród innych pochodzących od tej osoby informacji i oświadczeń woli. Niedopuszczalne jest też zawieranie klauzul zgody w treści regulaminów, gdzie osoba podająca swoje dane nie ma możliwości swobodnego jej wyrażenia.

Z uwagi na stwierdzone uchybienia w procesie przetwarzania danych osobowych, wobec Spółki zostało wszczęte postępowanie administracyjne. W toku postępowania Spółka usunęła uchybienia stanowiące przedmiot postępowania m.in. poprzez zapewnienie swobody w wyrażeniu zgody na przetwarzanie danych osobowych w celach marketingowych podmiotów trzecich oraz zgody na udostępnianie danych podmiotom trzecim, które będą je przetwarzały w celach marketingowych, a także zapewnienie, aby dane te były przetwarzane zgodnie z prawem. Z powyższych względów wszczęte wobec Spółki postępowanie administracyjne w tym zakresie zostało umorzone.

Kontroli został również poddany przedsiębiorca, który na podstawie informacji pozyskanych ze źródeł ogólnie dostępnych, jakim jest sieć Internet, stworzył bazę danych przeznaczoną do sprzedaży[79]. W toku kontroli stwierdzono m.in., że w odniesieniu do osób, które w trybie art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych zgłosiły sprzeciw wobec przetwarzania przez przedsiębiorcę (jako administratora danych) ich danych, podmiot ten przetwarzał dane w zakresie szerszym niż wskazany w przepisach ustawy o ochronie danych osobowych, tj. jej art. 32 ust. 3[80]. Natomiast przedsiębiorca wykraczając poza zakres dopuszczony przepisami prawa nadal przetwarzał dane osobowe takie jak nazwa podmiotu, numer telefonu i rodzaj prowadzonej działalności. W związku z powyższym Generalny Inspektor wszczął z urzędu postępowanie administracyjne w niniejszej sprawie, w celu wyjaśnienia okoliczności sprawy. W odpowiedzi na ww. zawiadomienie przedsiębiorca przesłał dowody potwierdzające, iż obecnie w odniesieniu do osób, które zgłosiły sprzeciw wobec przetwarzania ich danych osobowych przetwarza dane tych osób wyłącznie w zakresie i w celu wskazanym w art. 32 ust. 3 ustawy o ochronie danych osobowych, tj. w zakresie: imienia i nazwiska oraz adresu. Na tej podstawie postępowanie w sprawie w tym zakresie zostało umorzone[81].

[79] Kontrola DIS-K-421/178/14

[80] Art. 32.3. W razie wniesienia sprzeciwu, o którym mowa ust. 1 pkt 8, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

[81] Decyzja DIS/DEC-390/15/37284

Z kolei w toku kontroli przeprowadzonej w Spółce prowadzącej apteki ustalono, iż zamierzała ona prowadzić program polegający na udostępnieniu klientowi apteki należącej do Spółki możliwości posiadania konta w serwisie internetowym programu, za pośrednictwem którego miałby on dostęp do informacji, jakie produkty zakupi w ww. aptekach. Ponadto klient miałby możliwość wprowadzenia informacji o produktach zakupionych w innych aptekach oraz zamieszczać informacje o dowolnej treści dotyczące tych produktów.

Na życzenie klienta farmaceuta posiadałby dostęp do jego konta w momencie dokonania przez niego zakupu produktów w aptece Spółki. Mając dostęp do informacji o zakupionych wcześniej lekach farmaceuta mógłby w przypadku stwierdzenia, że właśnie kupowany lek wchodzi w interakcje z którymś z wcześniej zakupionych, poinformować o tym klienta.

Z wyjaśnień pracowników Spółki wynikało, iż farmaceuci mają obowiązek weryfikowania recept każdego dnia oraz wydanych na podstawie tych recept leków, czy nie nastąpiła pomyłka podczas wydawania leków. W przypadku stwierdzenia pomyłki farmaceuta miałby obowiązek skontaktowania się z pacjentem w celu jej naprawienia. Obecnie dokonuje tego albo za pośrednictwem zakładu opieki zdrowotnej, gdzie wystawiono receptę albo udając się osobiście pod adres pacjenta zamieszczony na recepcie. W momencie wprowadzenia programu farmaceuta mógłby sprawdzić poprzez numer PESEL, jeżeli będzie zamieszczony na recepcie, czy pacjent jest uczestnikiem programu, a jeżeli tak, mógłby zatelefonować na numer telefonu pacjenta znajdujący się na jego koncie. Farmaceuta posiadałby dostęp do informacji o produktach zakupionych w aptekach Spółki oraz produktach zakupionych w innych aptekach, o których informacje klient zamieści na swoim koncie. Miałby również możliwość zamieszczenia notatki dotyczącej danego produktu w momencie jego zakupu w aptece Spółki.

Jak ustalono w toku kontroli, w aptekach należących do Spółki były sprzedawane produkty, o których mowa w art. 86 ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne (Dz. U. z 2008 r. Nr 45, poz. 271 z późn. zm.) [82].

[82] Zgodnie z art. 86 ust. 1 ustawy Prawo farmaceutyczne, apteka jest placówką ochrony zdrowia publicznego, w której osoby uprawnione świadczą w szczególności usługi farmaceutyczne, o których mowa w ust. 2. W myśl art. 86 ust. 2 tejże ustawy nazwa apteka zastrzeżona jest wyłącznie dla miejsca świadczenia usług farmaceutycznych obejmujących: wydawanie produktów leczniczych i wyrobów medycznych, określonych w odrębnych przepisach; sporządzanie leków recepturowych, w terminie nie dłuższym niż 48 godzin od złożenia recepty przez pacjenta, a w przypadku recepty na lek recepturowy zawierający środki odurzające lub oznaczonej "wydać natychmiast" - w ciągu 4 godzin; sporządzenie leków aptecznych; udzielanie informacji o produktach leczniczych i wyrobach medycznych. Art. 72 ust. 5 Prawa farmaceutycznego stanowi, iż hurtownie farmaceutyczne mogą prowadzić obrót hurtowy: wyrobami medycznymi; produktami leczniczymi

Zdaniem Spółki prowadzenie programu jest sprawowaniem opieki farmaceutycznej, o której mowa w art. 2a ust. 1 ustawy z dnia 19 kwietnia 1991 r. o izbach aptekarskich (Dz. U. z 2014 r. poz.1429 z późn. zm.)[83], a w związku z tym podstawę prawną przetwarzania danych osobowych w ramach tego programu stanowi art. 23 ust. 1 pkt 2 ustawy[84] o ochronie danych osobowych w związku z ww. art. 2a ust. 1 ustawy o izbach aptekarskich.

W związku z wątpliwościami, czy realizację takiego programu można uznać za sprawowanie opieki farmaceutycznej, o której mowa powyżej, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do Głównego Inspektora Farmaceutycznego o wydanie opinii w tym zakresie.

W odpowiedzi Główny Inspektor Farmaceutyczny stwierdził[85], że opisany powyższej program nie stanowi formy opieki farmaceutycznej w rozumieniu ustawy o izbach aptekarskich. Przedmiotowy program nie zakłada dokumentowanej współpracy pomiędzy farmaceutą zatrudnionym w aptece Spółki a lekarzem, czy też przedstawicielem innego zawodu medycznego, co nie pozwala na zakwalifikowanie go jako formy sprawowania opieki farmaceutycznej. Z opisu programu wynika, że ma on przede wszystkim służyć do śledzenia historii zakupów dokonanych w sieci aptek Spółki, zaś od aktywności posiadacza konta zależy, czy w systemie znajdą się informacje o produktach nabytych w innych aptekach. Chodzi przy tym o zakupy wszelkiego rodzaju artykułów dostępnych w aptekach, nie tylko produktów leczniczych. Z kolei dodatkowa „usługa" polegająca na informowaniu przez farmaceutę o wzajemnym oddziaływaniu na siebie leków zakupionych przez klienta jest w istocie obowiązkiem każdego farmaceuty zatrudnionego w aptece. Wykonywanie zawodu

---

przeznaczonymi wyłącznie na eksport, posiadającymi pozwolenie na dopuszczenie do obrotu inne niż określone w ust. 3; środkami spożywczymi specjalnego przeznaczenia żywieniowego, suplementami diety, w rozumieniu przepisów o bezpieczeństwie żywności i żywienia; środkami kosmetycznymi, w rozumieniu art. 2 ustawy z dnia 30 marca 2001 r. o kosmetykach (Dz. U. Nr 42, poz. 473, z późn. zm.), z wyłączeniem kosmetyków przeznaczonych do perfumowania lub upiększania; środkami higienicznymi; przedmiotami do pielęgnacji niemowląt i chorych; środkami spożywczymi zawierającymi w swoim składzie farmakopealne naturalne składniki pochodzenia roślinnego; środkami dezynfekcyjnymi stosowanymi w medycynie - spełniającymi wymagania określone w odrębnych przepisach. Natomiast zgodnie z art. 86 ust. 8 ww. ustawy w aptekach ogólnodostępnych na wydzielonych stoiskach można sprzedawać produkty określone w art. 72 ust. 5 posiadające wymagane prawem atesty lub zezwolenia, pod warunkiem że ich przechowywanie i sprzedaż nie będą przeszkadzać podstawowej działalności apteki.

[83] Zgodnie z art. 2a ust. 1 ustawy wykonywanie zawodu farmaceuty ma na celu ochronę zdrowia publicznego i obejmuje udzielanie usług farmaceutycznych polegających w szczególności na sprawowaniu opieki farmaceutycznej polegającej na dokumentowanym procesie, w którym farmaceuta, współpracując z pacjentem i lekarzem, a w razie potrzeby z przedstawicielami innych zawodów medycznych, czuwa nad prawidłowym przebiegiem farmakoterapii w celu uzyskania określonych jej efektów poprawiających jakość życia pacjenta.

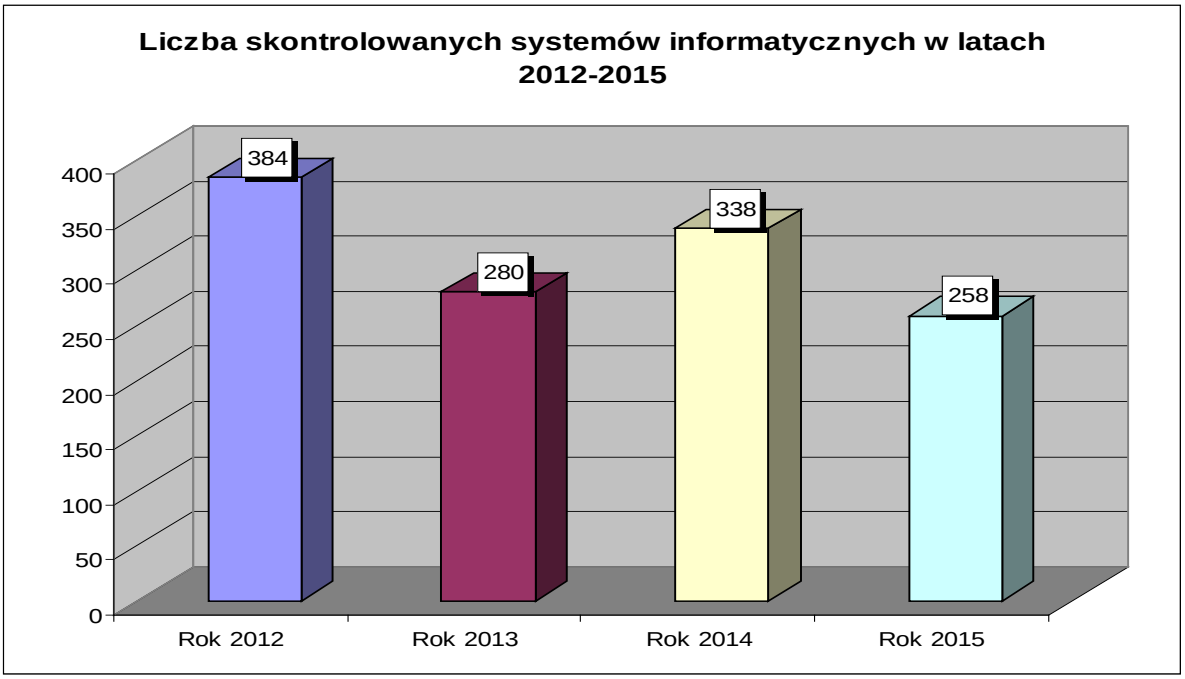
[84] Zgodnie z art. 23. ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanie danych jest dopuszczalne, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

[85] Pismo z dnia 2 marca 2016 r. nr GIF-P-L-076/59/SzP/16.

farmaceuty polega w szczególności na wydawaniu produktów leczniczych będących przedmiotem obrotu w aptekach (art. 2a ust. 1 pkt 3 ustawy o izbach aptekarskich), co nie jest tożsame z pozbawioną refleksji sprzedażą. Dodatkowo farmaceuta udziela informacji i porad dotyczących działania i stosowania produktów leczniczych wydawanych w aptece (art. 2a ust. 1 pkt 6 ustawy o izbach aptekarskich). Można zatem, jak wskazał Główny Inspektor Farmaceutyczny, wyprowadzić wniosek, że farmaceuta wydający lek ma obowiązek zweryfikowania, czy nie będzie on reagował z innymi zażywanymi przez pacjenta preparatami - niezależnie od jego uczestnictwa w programie. W konsekwencji, program wydaje się być narzędziem marketingowym, przedstawiającym realizację ustawowych obowiązków farmaceuty jako unikalną cechę aptek należących do Spółki.

2.3. Systemy informatyczne służące do przetwarzania danych osobowych.

W ramach przeprowadzonych w 2015 r. kontroli, weryfikacji poddano 258 systemów informatycznych wykorzystywanych do przetwarzania danych osobowych.



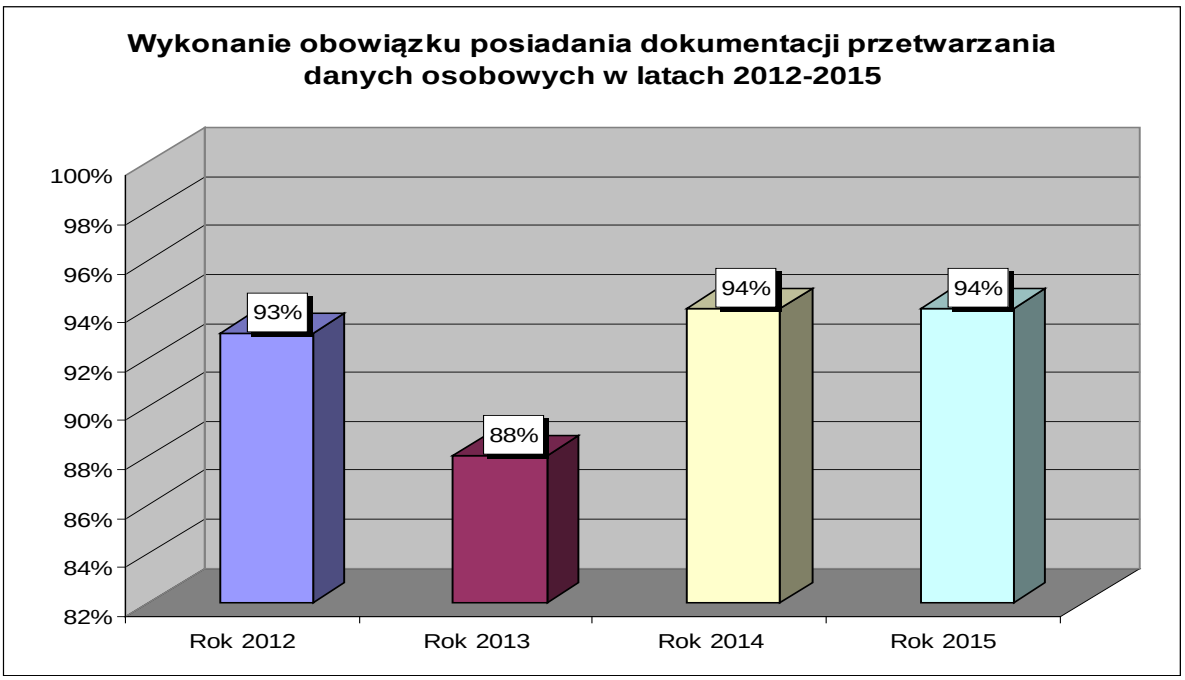
Wykres 2: ***Zestawienie porównawcze liczby skontrolowanych systemów informatycznych w latach 2012-2015.***

2.4. Wyniki kontroli w zakresie obowiązków formalnych i organizacyjnych.

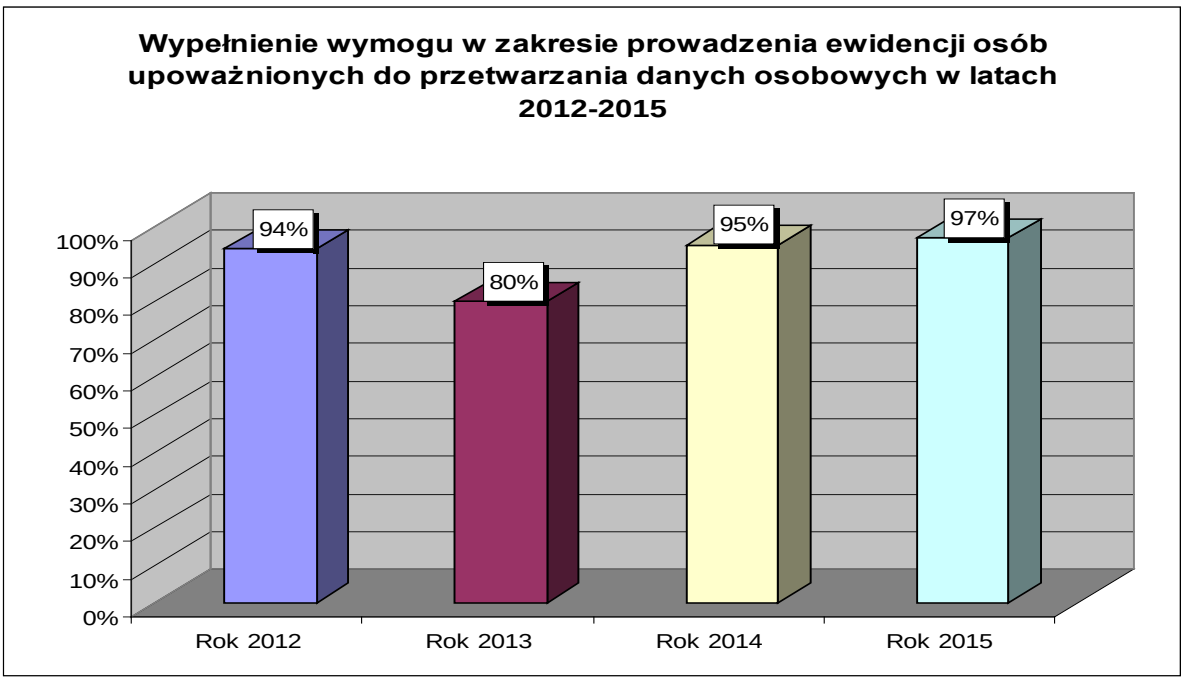
Spełnienie przez kontrolowane podmioty w latach 2012-2015 wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie i rozporządzeniu, zobrazowane zostało poniżej w formie wykresów. Pokazują one procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub w odniesieniu do ogólnej liczby kontrolowanych w danym roku systemów informatycznych. Zamieszczone informacje odnoszące się do prowadzonej dokumentacji procesu przetwarzania danych, czy obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, 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 w odniesieniu 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 2012-2015 przedstawiono na poniższych wykresach.



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

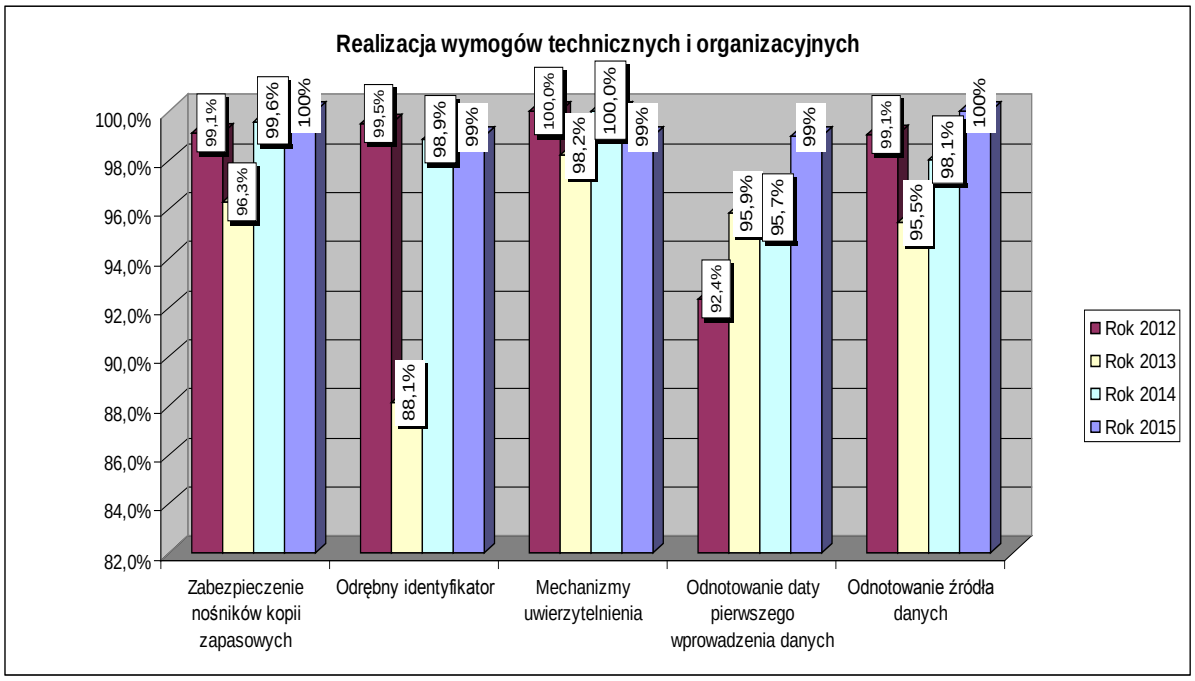


Wykres 4: ***Stopień realizacji obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.***

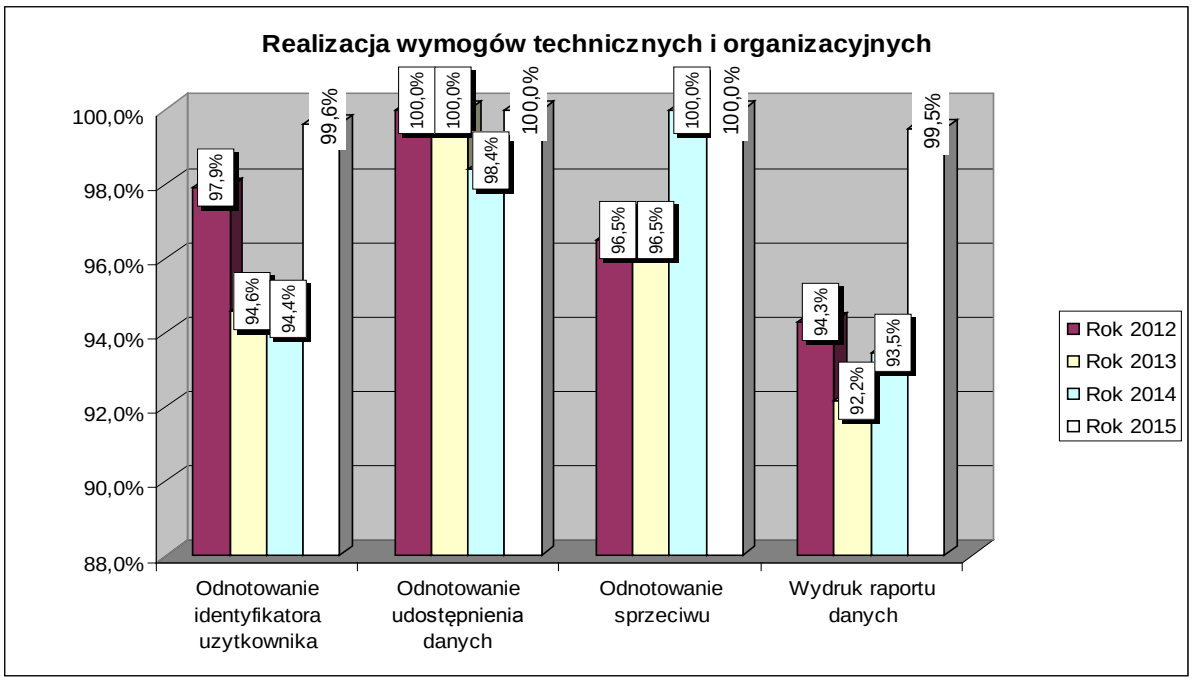
2.5. Wyniki kontroli w zakresie warunków techniczno-organizacyjnych

Skontrolowane w 2015 r. podczas czynności kontrolnych systemy informatyczne służące do przetwarzania danych osobowych, 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 za spełnione. Stopień realizacji wymogów o charakterze techniczno-organizacyjnym dla systemów informatycznych objętych kontrolą w roku 2015 w porównaniu do lat 2012-2014, przedstawiono na poniższych wykresach.



Wykres 5: ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2012-2015 – część I.***



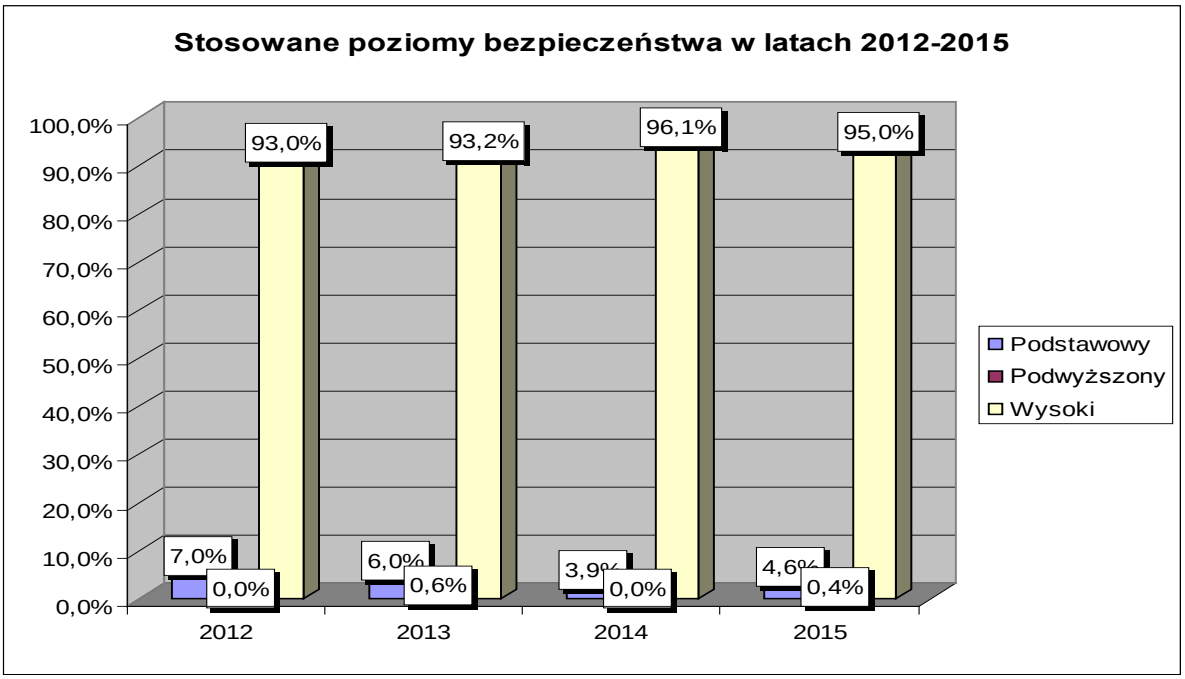
Wykres 6: ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2012-2015 – część II.***

Jak wynika z przedstawionych wykresów, liczba systemów informatycznych objętych kontrolą w roku 2015 była niższa niż w latach poprzednich. Wynikało to z faktu, że dane osobowe były przetwarzane w specjalistycznych systemach informatycznych oraz z tego, iż coraz większa liczba podmiotów powierza przetwarzanie danych osobowych innym podmiotom dysponującym własnymi systemami informatycznymi. 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 tj. 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 2015 roku, w porównaniu z rokiem poprzednim, można zaobserwować poprawę realizacji obowiązku dotyczącego konieczności stosowania odrębnych identyfikatorów oraz stosowania mechanizmów uwierzytelniania. Zapewnienie posiadania przez systemy informatyczne funkcjonalności związanych z odnotowywaniem informacji o dacie oraz

identyfikatorze użytkownika wprowadzającego dane, jak również możliwość sporządzenia raportów z ww. odnotowaniami, kształtuje się na poziomie zbliżonym do lat poprzednich.

Podział na poziomy bezpieczeństwa w odniesieniu do skontrolowanych w latach 2012 - 2015 r. systemów informatycznych przedstawiony został na poniższym wykresie.

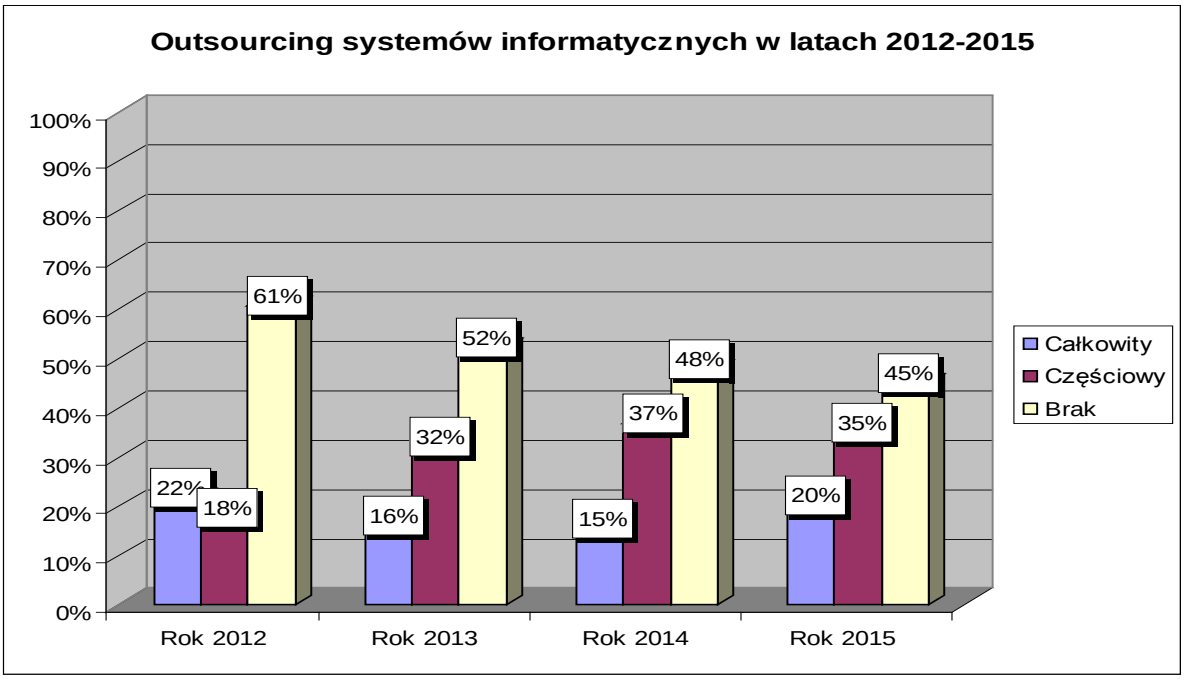


Wykres 7: ***Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych skontrolowanych w latach 2012-2015.***

Jak wynika z ww. wykresu, większość podmiotów skontrolowanych w 2015 r. (95%) zastosowała wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych. Stwierdzono niewielki wzrost poziomu zabezpieczeń na poziomie podstawowym. Wiąże się to z tym, że większość kontrolowanych w 2015 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 2015 r. czynności kontrolnych stwierdzono tylko jeden przypadek stosowania podwyższonego poziomu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

Jak wynika z przeprowadzonych w 2015 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

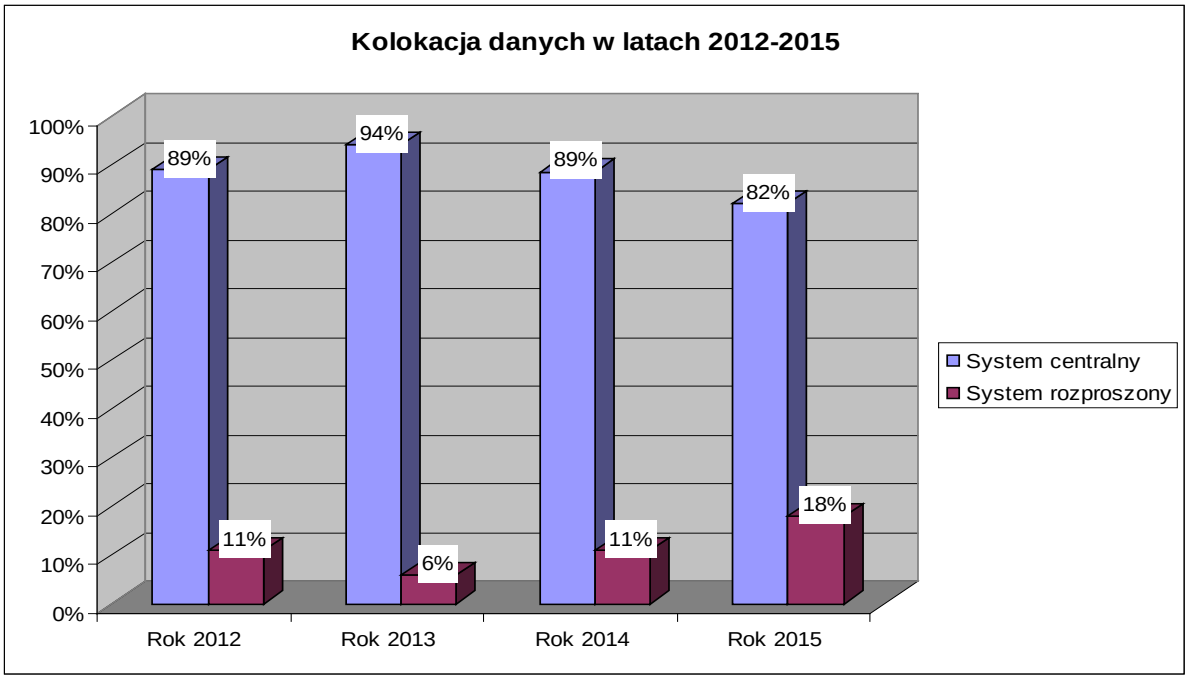
sprzęt teleinformatyczny administrator danych powierzył w całości do administrowania podmiotom zewnętrznym, w 2015 r. stosowany był w odniesieniu do około 20 % systemów informatycznych. Jest to liczba nieco większa niż w latach ubiegłych. W 2015 r. odnotowano również niewielki spadek liczby tych systemów informatycznych, których obsługą techniczną i administracją zajmowali się wyłącznie pracownicy administratora danych (45% systemów informatycznych). Na zbliżonym poziomie kształtuje się także 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 związanych z zarządzaniem bazą danych czy wykonywaniem kopii zapasowych, itp. Outsourcing częściowy stosowany był w 35% skontrolowanych w 2015 r. systemach.



Wykres 8: ***Ilościowy udział outsourcingu systemów informatycznych objętych kontrolami w latach 2012-2015.***

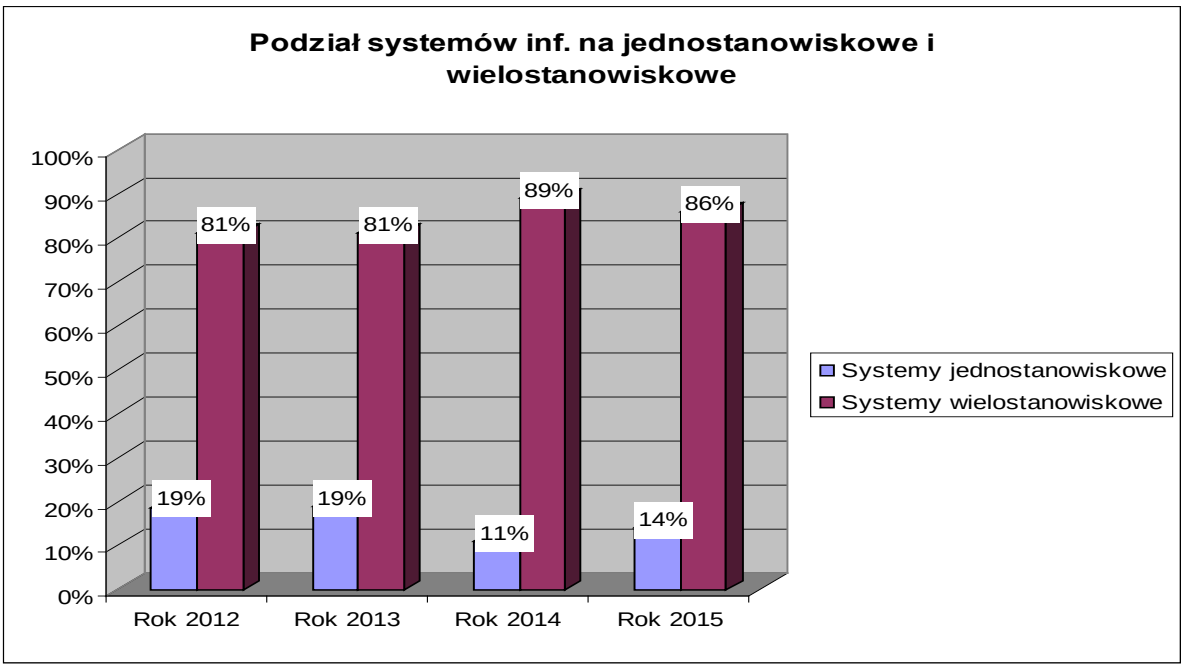
W większości skontrolowanych w 2015 roku podmiotów, dane osobowe zapisywane były w jednym, centralnym miejscu, np. na serwerze/serwerach znajdujących się w jednym budynku, zazwyczaj w siedzibie kontrolowanego podmiotu. Zauważyć jednak należy, że w stosunku do lat poprzednich zwiększyła się liczba podmiotów wykorzystujących do przetwarzania danych osobowych systemy rozproszone. Poniżej zilustrowano stopień

stosowania przez kontrolowane podmioty rozwiązań technicznych opartych o systemy centralne i rozproszone.



Wykres 9: ***Ilościowy udział centralnego/rozproszonego przetwarzania danych w systemach informatycznych objętych kontrolą w latach 2012 - 2015.***

Jak przedstawiono na powyższym wykresie w 2015 r. w porównaniu z latami 2012 - 2015 liczba wykorzystywanych wielostanowiskowych systemów informatycznych znajduje się na zbliżonym poziomie (86%). Rozwiązania oparte o systemy jednostanowiskowe stanowiły niecałe 14% skontrolowanych systemów informatycznych. Zastosowanie systemów jednostanowiskowych w większości przypadków dotyczyło użytkowanych przez dłuższy czas systemów informatycznych. Zauważyć jednak należy, że systemy jednostanowiskowe stosowano również w przypadkach, gdy wymagała tego specyfika ich zastosowania (np. systemy monitoringu).



Wykres 10: ***Procentowy udział systemów informatycznych jedno- i wielostanowiskowych wśród systemów objętych kontrolą w latach 2012-2015.***

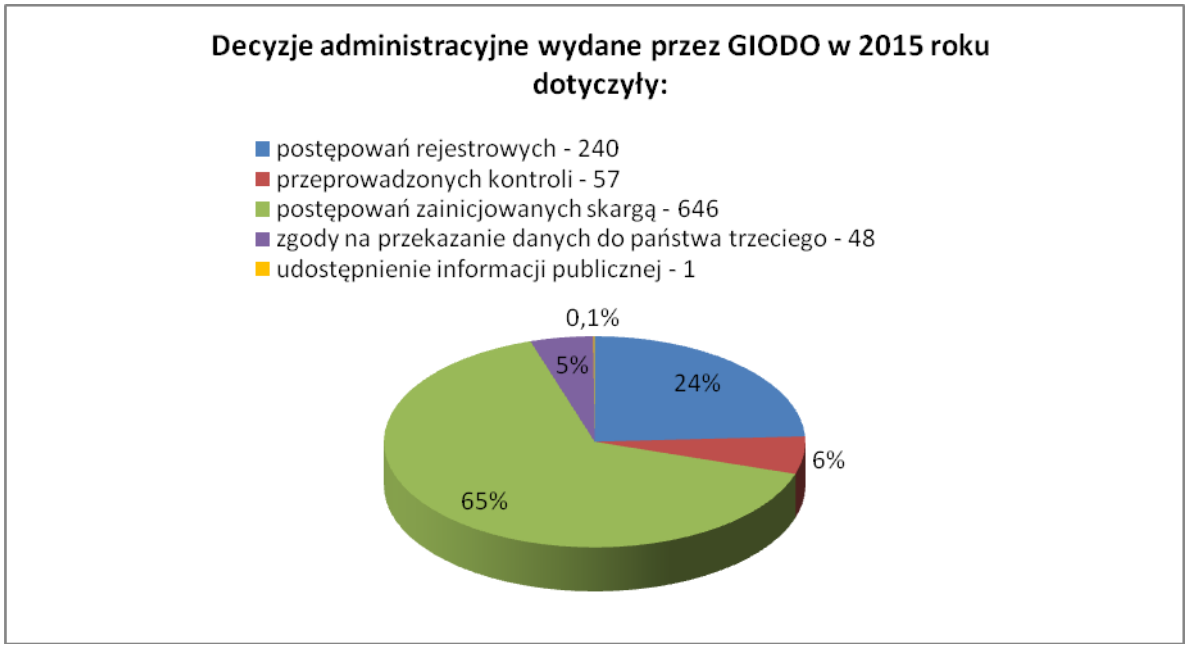
3. Wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych

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 (Dz. U. z 2016 r. poz. 23). 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 2015 r. Generalny Inspektor wydał **992 decyzje administracyjne,** tj. o 227 mniej w stosunku do roku 2014. Spośród 992 decyzji wydanych w 2015 r. **240 dotyczyło postępowań rejestrowych**, **57 zostało wydanych w związku z przeprowadzonymi kontrolami, 646**

wydano na skutek postępowania zainicjowanego skargą, 48 dotyczyło zgody na przekazanie danych do państwa trzeciego oraz **1 - udostępnienia informacji publicznej.**



Wykres 11: ***Liczbowe zestawienie rodzajów decyzji administracyjnych wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2015 r.***

3.2. Zawiadomienia o podejrzeniu popełnienia przestępstwa.

W analizowanym roku sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych skierował do organów powołanych do ścigania przestępstw **24 zawiadomienia o podejrzeniu popełnienia przestępstwa przez podmioty odpowiedzialne za przetwarzanie danych osobowych**. W porównaniu z rokiem 2014, w którym wystosowano 10 zawiadomień, stanowi to znaczny wzrost kierowanych do organów ścigania zawiadomień. **20 zawiadomień** złożonych zostało w związku z informacjami przekazanymi Generalnemu Inspektorowi przez podmioty indywidualne, zaś **4 zawiadomienia** złożonych zostało w związku z utrudnianiem wykonania czynności kontrolnych, co wyczerpuje znamiona czynu zabronionego, o którym mowa w **art. 54a ustawy o ochronie danych osobowych**. Należy w tym miejscu zaznaczyć, że na ogólną liczbę zawiadomień skierowanych do organów ścigania, pięć przypadków dotyczyło stwierdzonego przez organ w toku postępowania administracyjnego spenalizowanego w **art. 49 ust. 1 ustawy**, przetwarzania danych osobowych przez podmioty nieuprawnione, które przetwarzały te dane bez podstawy prawnej. Ponadto w trzech przypadkach zawiadomienia dotyczyły przestępstwa wskazanego w **art. 51 ustawy**, tj. udostępnienia danych osobowych podmiotom nieupoważnionym, czego przykładem jest sprawa, w której organ dokonał ustaleń, iż Skarżący otrzymywał na swoje

konto mailowe rachunki wystawiane przez Spółkę innej osobie[86]. Z kolei 4 zawiadomienia dotyczyły przestępstw wskazanych zarówno w **art. 51 i art. 52 ustawy** o ochronie danych osobowych, zaś w 3 innych sprawach Generalny Inspektor Ochrony Danych Osobowych skierował zawiadomienia o podejrzeniu popełnienia przestępstwa określonego w **art. 54 ustawy**, tj. niedopełnienia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazanie tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie. W dwóch przypadkach zawiadomienia zostały skierowane wobec podmiotu, który wprawdzie spełnił wobec Skarżących ww. obowiązek w momencie wszczęcia postępowania przed organem, ale po około 6 latach od pozyskania ww. danych[87].

Ponadto w 4 przypadkach skierowane zostały zawiadomienia o podejrzeniu popełnienia przestępstw określonych zarówno **w art. 49 i art. 54 ustawy o ochronie danych osobowych,** z czego w dwóch sprawach skierowane zostały zawiadomienia wobec tego samego podmiotu. Skarżący otrzymali pocztą elektroniczną potwierdzenie zawarcia z przedsiębiorcą umowy o uruchomienie usługi dostępu do płatnej sekcji serwisu internetowego oraz fakturę za rzekomo zawartą z nim umowę. Ponadto Skarżący na swoje elektroniczne skrzynki pocztowe otrzymali zaproszenia do korzystania ze strony internetowej prawniczego portalu edukacyjnego, którego regulamin zaakceptowali. Skarżący nie mieli świadomości, iż w ten sposób mogą zawrzeć umowę z przedsiębiorcą. Następnie Skarżący otrzymali na swoją elektroniczną skrzynkę pocztową informację, iż ich długi zostały opublikowane na internetowej giełdzie długów i jeżeli długi te nie zostaną skutecznie zbyte, system automatycznie roześle informację o nich do firm znajdujących się w okolicy Skarżących. Przedsiębiorca, jako administrator obu serwisów internetowych, nie zrealizował ciążącego na nim obowiązku informacyjnego z art. 25 ustawy o ochronie danych osobowych[88]. Podobnie zostało skierowane również kolejne zawiadomienie na ww. przedsiębiorcę w związku z okolicznościami wymienionym powyżej, lecz ponadto zarzucono mu jeszcze naruszenie **art. 53 ustawy o ochronie danych osobowych**, tj. niezgłoszenie do rejestracji zbioru danych[89].

[86] Zawiadomienie GIODO z dnia 16 czerwca 2015 r. DOLiS/ZAW-13/15/47819.
[87] Zawiadomienie GIODO z dnia 23 września 2015 r. DOLiS/ZAW-17/15/86809 oraz zawiadomienie GIODO z dnia 16 października 2015 r. DOLiS/ZAW-19/15/92230.
[88] Zawiadomienie GIODO z dnia 19 stycznia 2015 r. DOLiS/ZAW-1/15/3538 oraz zawiadomienie GIODO z dnia 29 maja 2015 r. DOLiS/ZAW-11/15/42694.
[89] Zawiadomienie GIODO z dnia 17 lipca 2015 r. DOLiS/ZAW-14/15/63889.

Podsumowując należy stwierdzić, że w porównaniu do poprzedniego okresu sprawozdawczego znacząco wzrosła liczba spraw, w których organ skierował zawiadomienia o podejrzeniu popełnienia przestępstwa.

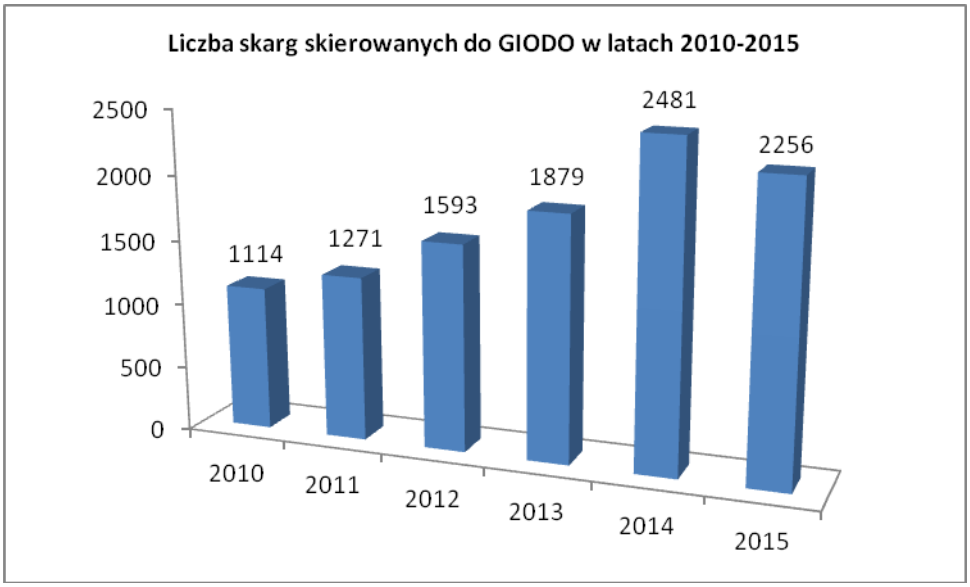
Liczbę zawiadomień o podejrzeniu popełnienia przestępstwa składanych przez Generalnego Inspektora w latach 2010-2015 przedstawia poniższy wykres:



Wykres 12: ***Porównanie liczby zawiadomień o podejrzeniu popełnienia przestępstwa skierowanych przez GIODO do organów ścigania w latach 2010–2015.***

3.3. Rozpatrywanie skarg

W 2015 r. do Departamentu Orzecznictwa, Legislacji i Skarg Biura GIODO wpłynęło **2256** skarg dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2014 liczba ta uległa **zmniejszeniu o 225.**

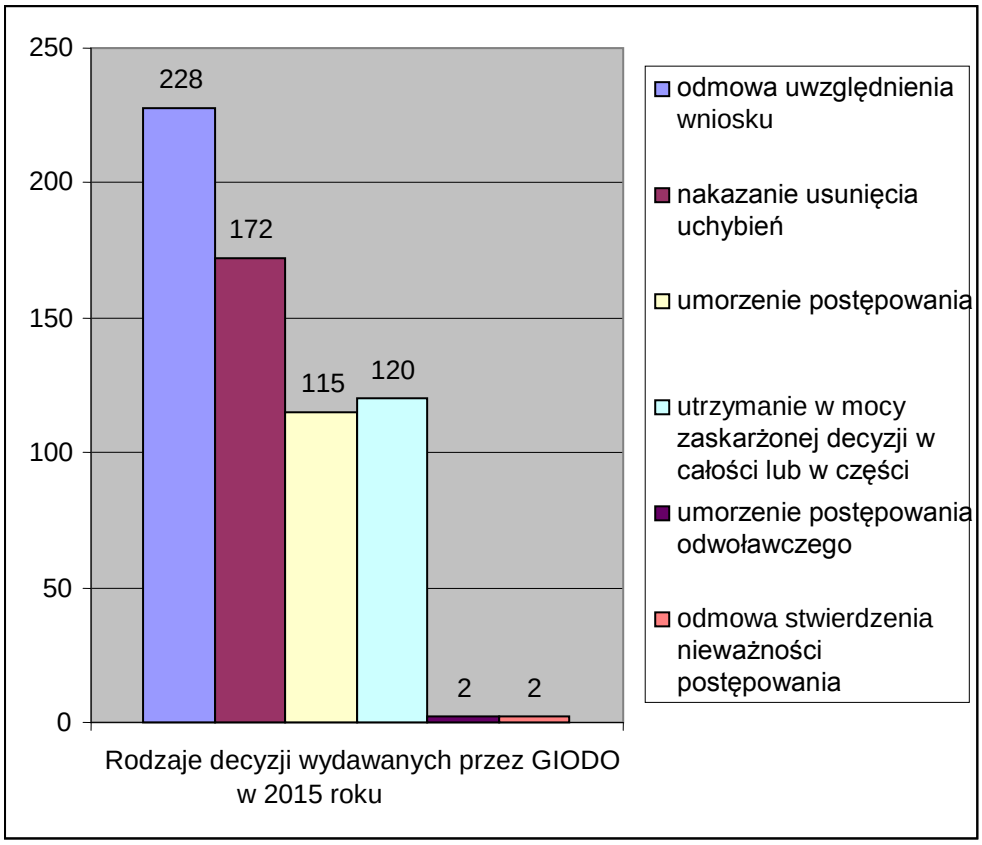


Wykres 13: ***Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2010–2015.***

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 2015 r. poz. 783 z późn. zm.). W sytuacji, gdy skarga nie spełniała warunków wymaganych przez ww. przepisy prawa, organ ochrony danych osobowych wzywał wnioskodawcę do uzupełnienia braków formalnych. Skutkiem powyższej analizy **95 skarg z 2015 r. zostało zwróconych do wnioskodawców**, zaś wiele skarg pozostało bez rozpoznania. W przypadku tych, które spełniały ww. warunki, 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 Generalny Inspektor Ochrony Danych Osobowych, w sprawach dotyczących skarg, w drodze decyzji administracyjnej **odmówił** uwzględnienia wniosku w **228** sprawach, **172** razy **nakazywał** przywrócenie stanu zgodnego z prawem, zaś w **115** przypadkach **umorzył** postępowanie administracyjne zainicjowane skargą.



Wykres 14: ***Zestawienie porównawcze rodzajów decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2015 r. w związku ze skargami.***

W **postępowaniu odwoławczym** wydano **129** decyzji, spośród których **120** razy GIODO **utrzymał** w mocy zaskarżone decyzje, w **7** sprawach **uchylał** decyzję w całości lub części, zaś w **2** przypadkach postępowanie odwoławcze zostało **umorzone.** Ponadto w 2 przypadkach wydane zostały decyzje o odmowie stwierdzenia nieważności decyzji organu. Dla porównania wskazać należy, iż w 2014 r. w postępowaniu odwoławczym wydano 107 decyzji, spośród których 92 razy utrzymano w mocy zaskarżone decyzje, 12 razy uchylone zostały decyzje, a w 3 przypadkach organ częściowo uchylił zaskarżone decyzje.

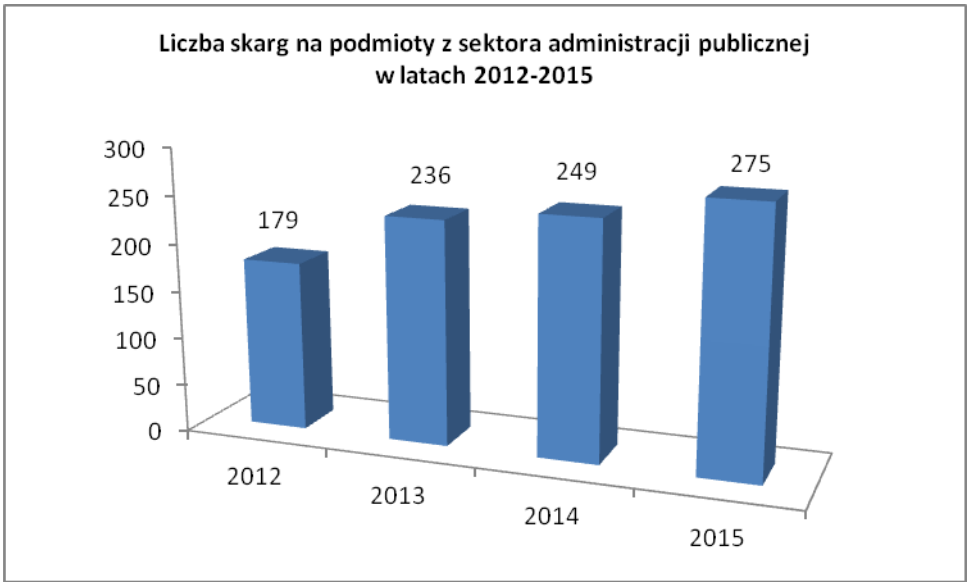
Analizując treść skarg wyróżnić należy 15 podstawowych kategorii, w zależności od zagadnień, których dotyczyły: 1) administracja publiczna, 2) bezpieczeństwo publiczne,

3) sądy, prokuratury, komornicy, 4) organizacje społeczne, 5) banki i inne instytucje finansowe, 6) Internet, 7) marketing, 8) mieszkalnictwo, 9) oświata i szkolnictwo wyższe, 10) służba zdrowia, 11) ubezpieczenia społeczne, majątkowe i osobowe, 12) telekomunikacja, 13) zatrudnienie, 14) windykacja, 15) inne.

Poniżej przedstawione zostały przykłady skarg, które wpłynęły w 2015 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych na podmioty działające w wybranych obszarach.

3.3.1. Administracja publiczna

W roku 2015 wpłynęło **275 skarg** dotyczących sektora **administracji publicznej**, tj. o 26 mniej niż w roku 2014. Jak w roku poprzednim, przeważająca liczba skarg dotyczyła 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 2012-2015.***

W omawianym okresie GIODO prowadził postępowanie w sprawie skargi na udostępnienie danych osobowych przez Prezydenta Miasta w rozdzielniku do pisma Prezydenta. Skarżący w treści swojej skargi wskazał, iż w piśmie będącym zawiadomieniem o wszczęciu postępowania w sprawie zatwierdzenia projektu budowlanego i udzielenia

pozwolenia na budowę Prezydent Miasta dopuścił się naruszenia przepisów poprzez umieszczenie w rozdzielniku pisma 239 imion i nazwisk wraz z prywatnymi adresami osób, do których zostało ono skierowane. Pismo to zostało również skierowane do inwestora. Po przeprowadzeniu postępowania wyjaśniającego Generalny Inspektor ustalił, iż przedmiotowe pismo inicjowało postępowanie administracyjne. Wprost przeciwnie do sytuacji, kiedy rozdzielnik załączany był do pisma podczas toczącego się postępowania administracyjnego. Osiągnięcie celu w postaci skutecznego poinformowania stron prowadzonego postępowania o podejmowanych w jego toku działaniach nie wymagałoby dołączania do każdego z pism wysyłanego do stron w toku tego postępowania listy innych osób, którym w postępowaniu tym również przysługuje status strony. Strony w toczącym się przed Prezydentem Miasta postępowaniu administracyjnym były uprawnione do zapoznawania się z faktem, iż zostało wszczęte postępowanie, którego są stroną oraz z danymi osobowymi identyfikującymi pozostałe strony. Wobec powyższego należało odmówić uwzględnienia wniosku Skarżącego[90].

W 2015 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w sprawie przetwarzania danych osobowych w zakresie adresów e-mail osób fizycznych przez posła na Sejm Rzeczypospolitej Polskiej, celem przesyłania przez niego drogą elektroniczną korespondencji o charakterze marketingu politycznego. Przedmiotowe maile zawierały przykładowo życzenia świąteczne, życzenia na Dzień Kobiet oraz materiały dotyczące działalności Ministerstwa Gospodarki i planowanych zmian w prawie. Minister Gospodarki w wyjaśnieniach złożonych przed Generalnym Inspektorem wskazał, iż baza adresów mailowych została stworzona w okresie prowadzenia przeze niego, jako osoby fizycznej, działalności społeczno-politycznej niemającej charakteru zarobkowego ani zawodowego. Zdaniem Ministra wysyłane przez niego materiały nie miały charakteru marketingowego, a tylko i wyłącznie informacyjny o zakresie szerszym niż pełniona przez niego funkcja. Związane one były z jego zainteresowaniami i zawierały informacje ważne ze społecznego i gospodarczego punktu widzenia. W ocenie Generalnego Inspektora Ochrony Danych Osobowych nie sposób było uznać przedmiotowego działania za przetwarzanie danych osobowych przez osobę fizyczną w celu osobistym, a było to przetwarzanie przez organ państwowy, czy też podmiot pełniący funkcje polityczne. Ponadto za nieuzasadnioną należy uznać argumentację o przetwarzaniu ww. danych wyłącznie w celach osobistych, bowiem w ocenie organu treść przesyłanych wiadomości i cel ich przesyłania, a przede wszystkim status ich nadawcy, przesądził o charakterze tych wiadomości jako marketingu politycznego. W związku z powyższym w drodze decyzji administracyjnej Generalny Inspektor nakazał usunięcie danych osobowych w zakresie

[90] Decyzja GIODO z dnia 03 lipca 2015 r. znak: DOLiS/DEC-556/15/58723,58727.

adresów e-mail osób fizycznych przetwarzanych dla celów wysyłania drogą elektroniczną korespondencji o charakterze marketingu politycznego[91]. Decyzja ta została wykonana.

3.3.2. Bezpieczeństwo publiczne

W analizowanym okresie do GIODO wpłynęły **43 skargi** dotyczących sektora **bezpieczeństwa publicznego**.

Większość skarg rozpatrywanych w tej dziedzinie dotyczyło przetwarzania przez Komendanta Głównego Policji danych osobowych w KSIP[92]. Wskazania wymaga, że zgodnie ze stanowiskiem zaprezentowanym przez sądy administracyjne, przepis art. 20 ust. 2a ustawy o Policji stanowi *lex specialis* w stosunku do przepisów ustawy o ochronie danych osobowych. W związku z powyższym 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. W tym miejscu należy podnieść, 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 Policji, o których mowa w art. 1 ust. 2 ustawy o Policji.

Przykładowo wskazać należy na skargę dotyczącą przetwarzania danych osobowych przez Komendanta Oddziału Żandarmerii Wojskowej. W treści skargi Skarżący podniósł, iż Żandarmeria Wojskowa bezprawnie pozyskała jego dane osobowe o stanie zdrowia, które zostały udostępnione jej przez pracownika Jednostki Woskowej. Komendant Oddziału Żandarmerii Wojskowej zwrócił się do Komendanta Wojewódzkiego Policji z wnioskiem o pozbawienie Skarżącego prawa do posiadania myśliwskiej broni palnej. Ponadto nieprawdziwie poinformował Policję, że Skarżący leczył się psychiatrycznie. Po przeprowadzeniu postępowania administracyjnego Generalny Inspektor odmówił uwzględnienia wniosku[93], a po złożeniu przez Skarżącego wniosku o ponowne rozpatrzenie sprawy, utrzymał w mocy zaskarżoną decyzję[94]. Podstawą pozyskania danych Skarżącego od Wojskowego Oddziału Gospodarczego dla celów wykonywania zadań Żandarmerii Wojskowej, był art. 29 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. W toku tych czynności Żandarmeria Wojskowa ujawniła możliwość wystąpienia okoliczności, o których mowa w art. 15 ust. 1 pkt 3 ustawy o broni i amunicji,

[91] Decyzja GIODO z dnia 09 listopada 2015 r. DOLiS/DEC-876/15/97600.
[92] Np. decyzja GIODO z dnia 30 stycznia 2015 r. znak: DOLiS/DEC-55/15/7003,7005.
[93] Decyzja GIODO z dnia 28 września 2015 r. DOLiS/DEC-781/15/87813,87816,87819,87821.
[94] Decyzja GIODO z dnia 17 grudnia 2015 r. DOLiS/DEC-961/15/106440,106442,106443,106444.

i mogła te informacje udostępnić Komendantowi Wojewódzkiemu Policji. Działanie takie było podjęte w ramach realizacji zadań Żandarmerii Wojskowej, określonych w art. 4 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. W ocenie Generalnego Inspektora Ochrony Danych Osobowych w sytuacji, gdy Żandarmeria Wojskowa ujawniła wobec Skarżącego okoliczności z art. 15 ust. 1 pkt 3 ustawy o broni i amunicji, to w ramach wykonywania zadania mającego na celu ochranianie miejsc publicznych i współdziałania ze służbami właściwymi w sprawach bezpieczeństwa i porządku publicznego, mogła informację dotyczącą Skarżącego udostępnić Komendantowi Wojewódzkiemu Policji, celem wszczęcia stosownego postępowania wyjaśniającego. Ponadto przetwarzanie danych Skarżącego przez Komendanta Wojewódzkiego Policji wskutek pozyskanych informacji od Żandarmerii, w celu przeprowadzenia stosownego postępowania administracyjnego w sprawie cofnięcia Skarżącemu pozwolenia na posiadanie broni palnej myśliwskiej do celów łowieckich, miało również swe oparcie w przepisach ustawy o broni i amunicji oraz ustawy o ochronie danych osobowych.

3.3.3. Sądy, prokuratura, komornicy

W 2015 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **58 skarg** dotyczących sektora **sądów, prokuratur i komorników**.

Jedna ze skarg dotyczyła przetwarzania danych osobowych przez Komorników, którzy przesłali do Spółki pisma o zajęciu wynagrodzenia za pracę Skarżącego, pomimo iż w tym czasie Skarżący nie był już jej pracownikiem. Z dowodów wynikało, iż kasa oszczędnościowa zwróciła się do Komorników, z wnioskami o wszczęcie egzekucji przeciwko dłużnikowi, wskazując m.in. dane osobowe Skarżącego w zakresie jego prawdopodobnego miejsca zatrudnienia, celem przeprowadzenia egzekucji m.in. z wynagrodzenia za pracę. W związku z powyższym ww. Komornicy skierowali do wskazanego przez wierzyciela miejsca zatrudnienia Skarżącego, tj. Spółki, pisma dotyczące zajęcia wynagrodzenia za prace oraz wierzytelności zasiłku chorobowego z wezwaniem do dokonywania potrąceń. W odpowiedzi na powyższe, Spółka skierowała do Komorników pisma z informacją, że Skarżący nie był już jej pracownikiem, a jedynie pozostawał w stosunku pracy we wskazanym przez nią okresie. W ocenie Generalnego Inspektora zastosowana w niniejszej sprawie praktyka Komorników, była nieprawidłowa[95]. Na komorniku sądowym bowiem, jako administratorze danych, ciąży, zgodnie z art. 36 ust. 1 ustawy – obowiązek zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zebraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem

[95] Decyzja GIODO z dnia 08 maja 2015 r. DOLiS/DEC-384/15/36483,36484,36485,36486.

ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Z obowiązkiem tym koresponduje regulacja zawarta w art. 26 ust. 1 ustawy, w świetle której administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i musi zapewnić, aby pozostające w jego posiadaniu dane były przetwarzane zgodnie z prawem. Wobec takiego brzmienia cytowanych przepisów za nieprawidłową uznać należało sytuację, w której komornik bez jednoznacznego wstępnego sprawdzenia przekazuje przetwarzane przez siebie dane osobowe (w tym także dane szczególnie chronione) podmiotowi, o którym posiada jedynie niepotwierdzoną żadnymi dokumentami informację, iż zatrudnia on dłużnika. W związku z powyższym Generalny Inspektor skierował również do Prezesa Sądu Rejonowego wystąpienie w którym zasygnalizował stwierdzone nieprawidłowości[96].

3.3.4. Organizacje społeczne

W roku sprawozdawczym 2015 wpłynęło do Biura GIODO **16 skarg** dotyczących **organizacji społecznych.**

W omawianym okresie organ do spraw danych osobowych wydał decyzję w sprawie przetwarzania danych osobowych córki Skarżącej przez pracownika Stowarzyszenia zajmującego się osobami z upośledzeniem umysłowym. Córka Skarżącej objęta była pomocą psychologiczną świadczoną przez Stowarzyszenie, ale w związku z niezadowoleniem rodziców ze sposobu prowadzenia terapii, Skarżąca w imieniu córki z niej zrezygnowała. W sprawie tej rezygnacji odbyła się rozprawa przed Sądem Rejonowym, na którą został powołany w charakterze świadka terapeuta zatrudniony przez Stowarzyszenie. Na potrzebę uczestnictwa w rozprawie, ale bez wiedzy swojego przełożonego, terapeuta wyniósł poza budynek Stowarzyszenia dokumentację medyczną zawierającą dane osobowe córki Skarżącej. W związku z powyższym Generalny Inspektor uznał, iż wyniesienie dokumentacji medycznej zawierającej dane osobowe na potrzebę stawiennictwa w sądzie stanowiło naruszenie zasad prawidłowego zabezpieczenia i przechowywania tej dokumentacji. Nie istnieją bowiem przepisy prawa uprawniające pracownika do takiego działania. Zachowanie terapeuty wywołało ryzyko udostępnienia danych osobowych nią objętych osobom nieupoważnionym. Jednakże z uwagi na fakt, iż z materiału dowodowego jednoznacznie wynikało, że bezprawne wyniesienie ww. dokumentacji miało charakter incydentalny, ale też nieodwracalny, Generalny Inspektor odmówił uwzględnienia wniosku Skarżącej[97]. Jednocześnie GIODO skierował do Przewodniczącego Zarządu Stowarzyszenia stosowane wystąpienie sygnalizujące stwierdzone nieprawidłowości[98].

[96] Pismo GIODO z dnia 08 maja 2015 r. DOLiS-440-936/14/SP/I/36482.
[97] Decyzja GIODO z dnia 06 maja 2015 r. DOLiS/DEC-369/15/35694,35698.
[98] Pismo GIODO z dnia 05 maja 2015 r. DOLiS-440-1743/13/KA/I/35677/15.

3.3.5. Banki i inne instytucje finansowe

W omawianym roku sprawozdawczym 2015, wpłynęło **329 skarg**, w których zakwestionowano legalność działań **banków i innych instytucji finansowych**, (dla porównania w roku 2014 było ich 354).

Generalny Inspektor prowadził postępowanie w sprawie przetwarzania danych osobowych Skarżącego dla celów marketingowych, które polegały na kierowaniu do niego informacji handlowych w internetowym serwisie transakcyjnym. Skarżący wskazał, iż nie wyraził zgody na otrzymywanie informacji handlowych drogą elektroniczną oraz wyraził sprzeciw wobec przetwarzania jego danych osobowych w celach marketingowych. Choć w pierwszej decyzji GIODO odmówił uwzględnienia wniosku Skarżącego[99], to jednak na skutek ponownego rozpatrzenia sprawy uchylił zaskarżoną decyzję i nakazał Bankowi przywrócenie stanu zgodnego z prawem, poprzez zaprzestanie przetwarzania danych osobowych Skarżącego w celu marketingu produktów lub usług własnych oraz innych podmiotów[100]. W ocenie GIODO informacje zawarte w internetowym serwisie transakcyjnym Banku o jego nowych produktach, stanowiły marketing Banku z uwagi na podkreślanie atrakcyjności i nakłanianie do skorzystania z tej oferty. W świetle powyższych rozważań za zasadne należało uznać, iż Bank przetwarzał dane osobowe Skarżącego w celach marketingowych pomimo złożonego przez niego sprzeciwu i niezbędne było wobec tego nakazanie zaprzestania tego przetwarzania, niezależnie od formy i technicznego sposobu reklamy.

Stanowisko takie prezentowane było również przez sądy administracyjne. Wojewódzki Sąd Administracyjny w Warszawie (WSA) w wyroku z dnia 9 października 2015 r. stwierdził, iż cyt.: „Jeśli bowiem po zalogowaniu do serwisu, klient ma możliwość zapoznania się z reklamą Banku, to świadczy to o tym, że Bank dokonuje operacji na jego danych osobowych w celach marketingowych. Dochodzi więc w takiej sytuacji do bezprawnego (wobec złożonego sprzeciwu klienta) przetwarzania jego danych osobowych”[101].

W 2015 r. Generalny Inspektor wydał również decyzję w sprawie przetwarzanie danych osobowych Skarżącego, w tym na niewypełnienie przez Bank obowiązku informacyjnego, o którym mowa w art. 33 ustawy o ochronie danych osobowych oraz udostępnienie jego danych osobowych na rzecz BIK. W toku postępowania Skarżący podniósł również, iż Bank przetwarza jego dane osobowe w celach marketingowych pomimo złożonego sprzeciwu. W toku postępowania organ ustalił, iż Bank udostępniał dane osobowe Skarżącego na rzecz BIK w celu ustalenia zdolności kredytowej Skarżącego i przygotowania dla niego oferty

[99] Decyzja GIODO z dnia 05 sierpnia 2015 r. DOLiS/DEC-642/15/71725,71731.
[100] Decyzja GIODO z dnia 16 grudnia 2015 r. DOLiS/DEC-960/15/106369,106376.
[101] Wyrok WSA w Warszawie z dnia 09 października 2015 r., sygn. akt II SA/Wa 40/15.

produktów kredytowych poprzez wysyłanie zapytań monitorujących. Wobec powyższego organ do spraw ochrony danych osobowych uznał, iż brak było podstaw prawnych dla takich działań Banku oraz BIK i nakazał obu podmiotom usunięcie danych osobowych przetwarzanych w związku z ww. zapytaniami monitorującymi[102].

Inna ze skarg dotyczyła odmowy usunięcia danych osobowych Skarżącego przetwarzanych przez Bank w sytuacji gdy Skarżący nie był klientem Banku. Skarżący wnioskował o udzielenie mu kredytu, jednak nigdy nie została zawarta umowa pomiędzy nim a Bankiem. Jednak pomimo braku ww. umowy Bank przetwarzał dane osobowe Skarżącego w celach archiwalnych i dowodowych. W związku z powyższym Generalny Inspektor za zasadne uznał nakazanie Bankowi usunięcia danych osobowych Skarżącego wobec braku podstawy prawnej do ich przetwarzania i uznał, iż działanie Banku byłoby przetwarzaniem danych Skarżącego na zapas[103].

W związku z zastrzeżeniami co do legalności przetwarzanych danych przez banki, skierowane zostały do Departamentu Inspekcji Biura GIODO propozycje kategorii podmiotów lub zagadnień, które należałoby uwzględnić w harmonogramie kontroli sektorowych na rok 2016, obejmujących kontrolę sektorową w bankach pod kątem wskazanych poniżej zagadnień[104]:

1) przetwarzania danych osobowych klientów banków w celach marketingowych w serwisie transakcyjnym banku (którego użytkownikiem jest klient) w sytuacji wniesienia sprzeciwu przez jego użytkownika;
2) kopiowanie dokumentów tożsamości klientów – legalność, adekwatność, okresy retencji danych osobowych, w tym przepisy Prawa bankowego czy rozporządzenia Ministra Finansów z dnia 27 marca 2007 r. w sprawie szczegółowego zakresu przetwarzanych informacji dotyczących osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów oraz trybu usuwania tych informacji (Dz. U. z 2007 r. Nr 56, poz. 373);
3) przetwarzanie danych osobowych w BIK i ZBP po ogłoszeniu upadłości konsumenckiej klienta banku, w tym dla oceny zdolności kredytowej i analizy ryzyka kredytowego z art. 105 ust. 3 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2015 r. poz. 128 z późn. zm.);
4) profilowanie klientów banków (podstawa prawna, obowiązek informacyjny);
5) dopuszczalność przetwarzania danych w ramach zapytań w sprawie byłych klientów przez banki w BIK S.A., w związku z toczącym się postępowaniem w GIODO;

[102] Decyzja GIODO z dnia 11 grudnia 2015 r. DOLiS/DEC-950/15/105291,105293,105294.
[103] Decyzja GIODO z dnia 10 lipca 2015 r. DOLiS/DEC-586/15/61404,61495.
[104] Pismo z dnia 15.01.2016 r. znak: DOLiS-424/29/15/KK/2635/16.

6) przetwarzanie danych klientów na potrzeby realizacji postanowień umowy Foreign Account Tax Compliance Act (FATCA) oraz ustawy z dnia 9 października 2015 r. o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA (Dz. U. z 2015 r. poz. 1712); w szczególności czy dane na potrzeby realizacji umowy nie były przez banki przetwarzane w innych celach.

3.3.6. Internet

W 2015 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **336 skarg** dotyczących **przetwarzania danych osobowych w Internecie**, co stanowiło spadek ich liczby o 70 w porównaniu do zeszłego roku. Skargi głównie dotyczyły nieuprawnionego udostępniania danych na różnych portalach internetowych, co w konsekwencji prowadziło do naruszenia praw podmiotów danych. Wartym podkreślenia jest, że w obliczu dynamicznego rozwoju nowoczesnych technologii, Internet daje możliwość nieograniczonego zestawiania danych publicznie dostępnych, co oznacza, że wiele informacji może zyskać przymiot danych osobowych bez nadmiernego kosztu i czasu.

Generalny Inspektor Ochrony Danych Osobowych prowadził m.in. postępowanie administracyjne w sprawie skargi o nakazanie usunięcia danych osobowych z wyników jednej z wyszukiwarek internetowych. Zgodnie z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r. (sygn. akt. C-131/12) cyt.: „(…) operator wyszukiwarki internetowej jest zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby, linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje, również w przypadku, gdy te imię i nazwisko czy też te informacje nie zostały uprzednio czy też jednocześnie usunięte z tych stron internetowych (…)". Postępowanie prowadzone było wobec Spółki mającej siedzibę na terytorium Rzeczpospolitej Polskiej. Jednocześnie z materiału dowodowego zgromadzonego w sprawie wynikało, że Skarżący nie wystąpił do Spółki z wnioskiem o usunięcie ww. linku z wyników wyszukiwarki. Powyższe oznacza, że skarga Skarżącego była przedwczesna. Jak wynikało z wyroku Trybunału Sprawiedliwości Unii Europejskiej i wytycznych Grupy Roboczej Artykułu 29 oraz art. 35 ust. 2 ustawy, skarga do organu ochrony danych osobowych przysługuje dopiero wówczas, gdy operator otrzymawszy umotywowany wniosek osoby, której dane dotyczą o usunięcie jej danych osobowych z wyników wyszukiwania, nie dopełni tego obowiązku. Dokonując oceny okoliczności Generalny Inspektor odmówił uwzględnienia wniosku Skarżącego, zaś w

odniesieniu do wyników wyszukiwania, które nie były już prezentowane w wyszukiwarce umorzył postępowanie[105].

Do danych osobowych przetwarzanych w wynikach wyszukiwania odniósł się również Naczelny Sąd Administracyjny, który w wyroku z dnia 9 kwietnia 2015 r. podniósł, iż za przetwarzanie danych osobowych może być uznane także ich pośrednie udostępnianie (np. poprzez przekierowanie do innej domeny internetowej), nawet jeżeli dany podmiot tymi danymi fizycznie nie dysponuje. Sąd ten podkreślił, iż nie może podlegać ochronie prawnej działanie podmiotów, które w sposób bezrefleksyjny dokonują świadomego odesłania do stron internetowych, które mogą naruszać chronione prawem polskim dane osobowe. Jeżeli przekierowanie takie nie łączy się z fizycznym posiadaniem danych udostępnionych na innej stronie internetowej, należy to uwzględniać w procesie oceny danego podmiotu jako przetwarzającego dane osobowe i nimi administrującego. Natomiast brak posiadania danych nie wyłącza samo przez się możliwości uznania danego podmiotu za ich administratora. Oczywiście nie jest tak, iż każde przekierowanie, czy stworzenie innych warunków do wyszukania danych przez jedną witrynę internetową w zasobach innej, będzie od razu mieścić się w ramach instytucji uregulowanych w ustawie o ochronie danych osobowych. Niemniej nie może być zgody na to, by każde przekierowanie, które nie wiąże się z posiadaniem danych chronionych prawem, z założenia traktować jako nienaruszające przepisów ustawy. Stan taki mógłby stanowić podstawę do omijania polskich przepisów o ochronie danych osobowych poprzez "wyprowadzanie" danych chronionych spod jurysdykcji krajowej np. poprzez zamieszczanie ich na serwerze zagranicznym, przy jednoczesnym tworzeniu odesłań do zasobów udostępnionych przez inny podmiot, dostępnych bez większego problemu na terenie kraju, czy z innego miejsca na świecie. Przetwarzaniem może być więc również odsyłanie do danych zgromadzonych w innym miejscu, jeżeli podmiot taki jest, bądź powinien być świadomy, że odsyła do informacji, które podlegają ochronie[106].

Inna ze spraw dotyczyła usunięcia danych osobowych Skarżącej w zakresie imienia i nazwiska z adresu utworzonej i administrowanej przez byłego partnera Skarżącej strony internetowej. Skarżąca wskazała, iż ww. strona internetowa została wypozycjonowana w ten sposób, iż pojawiała się jako pierwsza w wynikach wyszukiwania. Po przeprowadzeniu postępowania administracyjnego w sprawie Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną, mocą której odmówił uwzględnienia wniosku Skarżącej[107]. Jednak po ponownym rozpatrzeniu sprawy na skutek odwołania Skarżącej ww. decyzja została uchylona i organ nakazał usunięcie danych osobowych Skarżącej w zakresie jej imienia i nazwiska z adresu utworzonej i administrowanej przez byłego

[105] Decyzja GIODO z dnia 09 października 2015 r. DOLiS/DEC-815/15/90625,90631.
[106] Wyrok NSA z dnia 09 kwietnia 2015 r. sygn. akt I OSK 2926/13.
[107] Decyzja GIODO z dnia 6 maja 2014 r. DOLiS/DEC-428/14/34413,34414.

partnera Skarżącej strony internetowej[108]. W ocenie Generalnego Inspektora dane zawarte w adresie strony internetowej stanowiły dane osobowe Skarżącej w zakresie jej imienia, pierwszego członu nazwiska oraz miejscowości miejsca zamieszkania. Zdaniem organu człon tego adresu wypełniał dyspozycję art. 6 ust. 1 ustawy o ochronie danych osobowych, gdyż są to informacje dotyczące możliwej do zidentyfikowania osoby fizycznej. Bowiem przy pomocy wyszukiwarki internetowej można, po wpisaniu do niej frazy imienia i nazwiska oraz miasta zamieszkania, dotrzeć - w sposób nie wymagający podjęcia nadmiernych działań i stosunkowo szybko - do innych danych Skarżącej, to jest do jej pełnego adresu zamieszkania oraz rodzaju wykonywanej działalności gospodarczej, numeru NIP i REGON. To z kolei pozwalało na pełną identyfikację osoby wskutek powiązania wyszukanych informacji ze sobą. Tego rodzaju powiązanie informacji pozwalało na przypisanie do Skarżącej dodatkowych informacji o jej przeszłości, o jej życiu prywatnym, epizodzie z życia uczuciowego, które dodatkowo ją dookreślają. Zauważyć jednocześnie należy, iż w przedmiotowej sytuacji nie można było mówić o celu wyłącznie osobistym przetwarzania danych osobowych Skarżącej z uwagi na fakt, iż jej dane zostały udostępnione w miejscu powszechnie dostępnym, jakim jest sieć Internet.

3.3.7. Marketing

W analizowanym okresie do GIODO wpłynęło **95 skarg** na podmioty działające w sektorze **marketingu.** Dla porównania w 2014 r. wpłynęły 153 skargi dotyczące tego zakresu. Większość skarg kierowanych do organu ochrony danych osobowych dotyczyła przetwarzania danych osobowych w celach marketingowych pomimo złożonego przez osoby, których dane dotyczą, sprzeciwu wobec takiego działania.

Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie w sprawie przetwarzania danych osobowych Skarżącego, w tym numeru telefonu, w celach marketingowych przez jednego z operatorów telekomunikacyjnych. Skarżący wskazał, iż przy przenoszeniu numeru telefonu od jednego operatora do drugiego zaznaczył, iż nie wyraża zgody na przetwarzanie jego danych w celach marketingowych. Pomimo tego otrzymywał smsy o charakterze marketingowym. W związku z powyższym Skarżący skierował do Spółki sprzeciw wobec przetwarzania jego danych osobowych w celach marketingowych. W toku postępowania wyjaśniającego Spółka przyznała, że przetwarzanie danych osobowych Skarżącego w celach marketingowych spowodowane było niezarejestrowaniem w systemach braku zgody przez konsultanta Spółki oraz nieprzekazaniem Spółce przez konsultanta firmy prowadzącej działania marketingowe informacji o wyrażeniu sprzeciwu. W ocenie GIODO nieprawidłowe przetwarzanie danych osobowych spowodowane niedopełnieniem obowiązku

[108] Decyzja GIODO z dnia 19 czerwca 2015 r. DOLiS/DEC-508/15/49447,49448.

rejestracji braku zgody oraz sprzeciwu przez konsultantów stanowiło naruszenie zasad legalnego przetwarzania danych osobowych w rozumieniu ustawy o ochronie danych osobowych. Niemniej jednak, ze względu na stanowisko Spółki, która oświadczyła, że ostatecznie blokada na dostarczenie elektronicznej informacji handlowej i komunikacji głosowej została uruchomiona, brak było podstaw do nakazania przez Generalnego Inspektora przywrócenia stanu zgodnego z prawem na podstawie art. 18 ust. 1 ustawy[109]. Ponadto w związku ze stwierdzeniem naruszenia przepisów ustawy o ochronie danych osobowych, tj. przetwarzania danych osobowych Skarżącego w celach marketingowych pomimo niewyrażenia przez niego zgody, a następnie złożenia przez niego sprzeciwu, Generalny Inspektor Ochrony Danych Osobowych, korzystając z uprawnień przewidzianych w art. 19a ustawy o ochronie danych osobowych, skierował do Spółki pisemne wystąpienie, w którym zasygnalizował stwierdzone nieprawidłowości i konieczność zmiany przez Spółkę dotychczasowej praktyki[110].

3.3.8. Mieszkalnictwo

W 2015 roku do Biura GIODO wpłynęło **81 skarg** dotyczących zagadnień związanych z **mieszkalnictwem,** co stanowi spadek ich liczby w stosunku do poprzedniego roku. W grupie tych zagadnień przede wszystkim znajdowały się skargi dotyczące przetwarzania danych osobowych skarżących przez spółdzielnie mieszkaniowe i wspólnoty mieszkaniowe.

Generalny Inspektor prowadził postępowanie w sprawie skargi na odmowę udostępnienia przez spółdzielnię mieszkaniową informacji o numerze księgi wieczystej lokalu mieszkalnego. Skarżący wskazali, że jako wierzyciele zamierzają wnieść przeciwko swojemu dłużnikowi postępowanie spadkowe po zmarłym ojcu, a w tym celu musi uzyskać informacje dotyczące własności tego lokalu. Wskazali też, że przeciwko dłużnikowi posiadają tytuł wykonawczy. Wobec odmowy udostępnienia przez spółdzielnię ww. danych, Skarżący wnieśli o wydanie przez Generalnego Inspektora Ochrony Danych Osobowych nakazu udostępnienia przez spółdzielnię na ich rzecz wnioskowanych informacji. Po przeprowadzeniu postępowania w sprawie organ wydał decyzję nakazującą udostępnienie wnioskowanych przez nich danych[111]. Generalny Inspektor uznał, iż żądanie Skarżących o udostępnienie ww. danych osobowych było w pełni uzasadnione i wypełniało dyspozycję art. 23 ust. 1 pkt 5 ustawy. Wniosek złożony przez Skarżących spełniał przesłanki udostępnienia danych, ponieważ został złożony do administratora danych w formie pisemnej, był właściwie umotywowany, wskazywał zakres i przeznaczenie oraz w sposób wiarygodny uzasadniał potrzebę ich udostępnienia. W ocenie Generalnego Inspektora wykorzystanie

[109] Decyzja GIODO z dnia 14 września 2015 r. DOLiS/DEC-751/15/83648,83657.
[110] Pismo GIODO z dnia 14 września 2015 r. znak: DOLiS-440-94/15/AD/I/83640.
[111] Decyzja GIODO z dnia 10 lipca 2015 r. DOLiS/DEC-585/15/61414,61416,61417.

danych w celu realizacji konstytucyjnie przysługującego prawa do dochodzenia swoich praw w drodze procesu sądowego nie może być uznane za naruszenie praw i wolności osób, których dane dotyczą. Prawo do prywatności nie ma bowiem charakteru absolutnego, a jego ochrona nie może odbywać się kosztem braku poszanowania praw innych osób.

W tym miejscu wskazać należy na postępowanie zakończone postanowieniem GIODO o odmowie wszczęcia postępowania w sprawie skargi spółdzielni mieszkaniowej dotyczącej naruszenia przez Urząd m.st. Warszawy obowiązku zachowania w tajemnicy danych osobowych członków spółdzielni[112]. W uzasadnieniu ww. postanowienia organ podniósł, iż spółdzielnia nie posiadała przymiotu strony przedmiotowego postępowania. Prawo do ochrony danych osobowych przysługuje bowiem tylko osobie, o której dane chodzi. Przepisy ustawy – Prawo spółdzielcze nie upoważniają zaś spółdzielni do wykonywania prawa ochrony danych osobowych w zastępstwie jej członków. Tym samym podmiot ten nie może skutecznie zainicjować tego postępowania. Ww. postanowienie zostało zaskarżone przez spółdzielnię mieszkaniową do Wojewódzkiego Sądu Administracyjnego w Warszawie, który w wyroku z dnia 24 lutego 2014 r. (sygn. akt. II SA/Wa 2249/13) uchylił ww. orzeczenia oraz stwierdził, że zaskarżone postanowienie nie podlega wykonaniu w całości. Od powyższego wyroku GIODO złożył skargę kasacyjną, która została uwzględniona w wyroku Naczelnego Sądu Administracyjnego[113]. W wyroku tym NSA za chybione uznał stanowisko WSA i w pełni podzielił zdanie GIODO. W szczególności wskazał, iż cyt.: „Odmawiając wszczęcia postępowania administracyjnego w przypadku gdy żądanie pochodzi od podmiotu niebędącego stroną, organ w ogóle nie rozważa kwestii ewentualnego wszczęcia danego postępowania z urzędu. Niezależnie od faktu, że jest to autonomiczna decyzja organu, to przede wszystkim muszą istnieć przesłanki do wszczęcia takiego postępowania, których rozważenie nie może dokonywać się w ramach oceny czy podmiot zgłaszający żądanie ma przymiot strony".

Ponadto Generalny Inspektor prowadził postępowanie w sprawie skargi na przetwarzanie danych osobowych Skarżącego przez byłego prezesa wspólnoty mieszkaniowej. W treści skargi Skarżący opisał działania byłego prezesa wspólnoty polegające na zleceniu sporządzenia rozliczenia zaliczek pobranych na poczet zarządu nieruchomością wspólną przez licencjonowaną księgową. W ocenie Skarżącego były prezes wspólnoty podejmując współpracę z księgową działał w imieniu własnym, tym samym przekazując konieczne do wykonania rozliczeń dokumenty zawierające dane osobowe Skarżącego udostępnił je na rzecz osoby nieupoważnionej. Generalny Inspektor Ochrony Danych Osobowych po przeprowadzeniu postępowania administracyjnego wydał decyzję administracyjną, mocą której odmówił uwzględnienia wniosku Skarżącego[114]. Skarżący złożył wniosek o ponowne

[112] Postanowienie GIODO z dnia 23 kwietnia 2013 r. DOLiS/POST-111/13/25204 oraz Postanowienie GIODO z dnia 27 września 2013 r. DOLiS/POST-291/13/63537.
[113] Wyrok NSA z dnia 10 grudnia 2015 r. sygn. akt I OSK 1613/14.
[114] Decyzja GIODO z dnia 15 września 2014 r. DOLiS/DEC-901/14/71790,71793.

rozpatrzenie sprawy. W odniesieniu do zarzutu Skarżącego dotyczącego udostępnienia jego danych osobowych osobom nieupoważnionym ustalono, że były prezes wspólnoty, działając na jej rzecz, zawarł umowę cywilnoprawną. W celu wykonania przedmiotu umowy tj. rozliczenia zaliczek pobranych od członków wspólnoty została zawarta umowa powierzenia przetwarzania danych osobowych, w tym danych osobowych Skarżącego. W kontekście przepisów ustawy działanie polegające na powierzeniu do przetwarzania danych osobowych innemu podmiotowi jest prawnie dopuszczalne. W ocenie Generalnego Inspektora umowa łącząca wspólnotę i przedsiębiorstwo finansowe, zarówno z uwagi na jej formę (pisemna), jak i treść (określenie celu, dla realizacji którego dane miały być przetwarzane, tj. w zakresie obsługi księgowej) odpowiadała wymogom określonym w art. 31 ustawy. Organ nie znalazł podstaw, aby kwestionować ww. umowę, co było przedmiotem żądania Skarżącego. W związku z powyższym po ponownym przeanalizowaniu materiału dowodowego zgromadzonego w sprawie Generalny Inspektor utrzymał w mocy zaskarżoną decyzję[115].

3.3.9. Oświata

W omawianym okresie do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **47 skarg** dotyczących **oświaty**.

Generalny Inspektor prowadził również postępowanie w sprawie o nakazanie dyrektorowi poradni psychologiczno-pedagogicznej udostępnienia na rzecz Skarżącego wszelkich danych osobowych jego małoletniego syna, które miały znajdować się w jego dokumentacji sporządzonej przez ten podmiot w związku z działaniami ww. poradni podjętymi wobec małoletniego. Dyrektor poradni w toku postępowania wyjaśniającego wskazał, iż syn Skarżącego nie pozostaje pod opieką poradni. Dokumentacja syna Skarżącego została przesłana zgodnie z rozporządzeniem MEN z dnia 16 lipca 2009 Dz. U. nr 116, poz. 977 do ośrodka terapii, który przejął opiekę nad synem Skarżącego zgodnie z postanowieniem Sądu. W związku z powyższym, wobec faktu, iż Poradnia nie przetwarzała danych osobowych Skarżącego ani jego małoletniego syna, Generalny Inspektor umorzył postępowanie[116].

3.3.10. Służba zdrowia

W 2015 roku do Biura GIODO wpłynęło **59 skarg** na podmioty działające w sektorze dotyczącym **służby zdrowia**, co stanowi 12 skarg więcej niż w roku ubiegłym.

Generalny Inspektor Ochrony Danych Osobowych prowadził postępowanie administracyjne w sprawie skargi na przetwarzanie danych osobowych Skarżącego przez stomatologa, z którym Skarżący pozostawał w sporze. Skarżący nie był pacjentem tego

[115] Decyzja GIODO z dnia 15 maja 2015 r. DOLiS/DEC-413/15/38485,38492.
[116] Decyzja GIODO z dnia 09 października 2015 r. DOLiS/DEC-814/15/90615,90618.

stomatologa, lecz jego wspólniczki. Jak wskazał Skarżący jego dane osobowe zawarte w karcie pacjenta zostały przekazane do Okręgowego Rzecznika Odpowiedzialności Zawodowej przy Okręgowej Izbie Lekarskiej przez ww. stomatologa. Rzecznik przetrzymywał te dane bez wiedzy i zgody Skarżącego. W toku postępowania wyjaśniającego ustalono, iż stomatolog jako wspólnik spółki cywilnej, był uprawniony do dostępu do dokumentacji stomatologicznej Skarżącego. Pomimo bowiem tego, że Skarżący nie był jej pacjentem, a jego dokumentacja przechowywana była w przychodni, to stomatolog, jako każdy z równoprawnych wspólników przychodni prowadzonej w formie spółki cywilnej, był administratorem danych osobowych Skarżącego. Jeśli zaś chodzi o przekazanie karty leczenia stomatologicznego Skarżącego przez stomatologa do Rzecznika, było to związane z kwestią dowodową w postępowaniu wyjaśniającym przed Rzecznikiem, które to postępowanie było zainicjowane skargą Skarżącego. Niemniej jednak – jak wskazał Rzecznik – karta ta nigdy nie była dołączona do akt przedmiotowego postępowania. W związku z powyższym Generalny Inspektor uznał, iż przetwarzanie danych osobowych Skarżącego przez stomatologa odbywało się zgodnie z prawem, tzn. w oparciu o przepisy ustawy Kodeks cywilny oraz ustawy o izbach lekarskich, czyli na podstawie art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych i w związku z tym odmówił uwzględnienia wniosku[117].

3.3.11. Ubezpieczenia społeczne, majątkowe i osobowe

W sektorze **ubezpieczeń społecznych, majątkowych i zdrowotnych** można zauważyć, że liczba skarg kierowanych do Generalnego Inspektora nie uległa znaczącej zmianie**.** W 2015 r. do Biura GIODO wpłynęło **55 skarg** (dla porównania w 2014 r. było ich 63). W tej grupie stwierdzić można, że we wszystkich kategoriach wpływały skargi w zbliżonej ilości i dotyczyły one nieprawidłowości w procesie przetwarzania danych osobowych, polegające m.in. na przesyłaniu przez towarzystwa ubezpieczeniowe dokumentów dotyczących umowy ubezpieczenia osobom nieupoważnionym.

Dla przykładu, w okresie sprawozdawczym organ do spraw ochrony danych osobowych prowadził postępowanie zakończone wydaniem decyzji administracyjnej w sprawie nieprawidłowości w procesie przetwarzania danych osobowych Skarżącego przez towarzystwo ubezpieczeniowe, w tym na udostępnienie jego danych osobowych osobom nieupoważnionym oraz niespełnienie wobec niego obowiązku informacyjnego wynikającego z art. 24 i 33 ustawy o ochronie danych osobowych. W toku postępowania dokonano ustaleń, iż pracownik towarzystwa ubezpieczeniowego, nie dokonał weryfikacji adresu email Skarżącego przed wysłaniem dokumentów ubezpieczenia Skarżącego. W związku z powyższym dokumenty te zostały wysłane na adres email agenta ubezpieczeniowego,

[117] Decyzja GIODO z dnia 09 kwietnia 2015 r. DOLIS/DEC-316/15/28676,28678,28683,28686,28687.

za pośrednictwem którego zawierana była jedna z poprzednich umów ubezpieczenia. W niniejszej sprawie ww. agent, na rzecz którego udostępnione zostały dane osobowe Skarżącego, nie był agentem z którym Skarżący tę umowę zawierał, a więc w odniesieniu do tej konkretnej sytuacji nie był on osobą upoważnioną do przetwarzania danych osobowych Skarżącego. Jednocześnie z uwagi na fakt, iż ww. zdarzenie było działaniem jednorazowym i działania takie nie były już kontynuowane, Generalny Inspektor Ochrony Danych Osobowych odmówił uwzględnienia wniosku[118]. Ponadto korzystając z uprawnienia przyznanego w art. 19 a ustawy, GIODO zwrócił się do prezesa zarządu towarzystwa ubezpieczeniowego o respektowanie przepisów o ochronie danych osobowych[119].

3.3.12. Telekomunikacja

W rozpatrywanych w 2015 r. sprawach dotyczących **telekomunikacji** do Biura GIODO wpłynęło **135 skarg.** Skargi te dotyczyły przetwarzania danych osobowych przez operatorów telekomunikacyjnych.

Podobnie jak w poprzednich latach Generalny Inspektor Ochrony Danych Osobowych utrwalił swoje stanowisko w przedmiocie wydawania operatorom telekomunikacyjnych nakazów udostępnienia na rzecz straż gminnych danych osobowych abonentów, wobec których prowadzone są postępowania wyjaśniające[120]. Straże gminne, w świetle przepisów prawa, wykonują zadania w zakresie ochrony porządku publicznego. Do wypełnienia zadań realizowanych dla dobra publicznego niezbędne jest ustalenie sprawcy wykroczenia, a następnie skierowania do sądu wniosku o ukaranie. Dobro publiczne jest wartością, którą operatorzy telekomunikacyjni bez wątpienia powinni brać pod uwagę w kontekście realizacji obowiązku ochrony danych abonenta na gruncie przepisów ustawy Prawo telekomunikacyjne.

Stanowisko GIODO znajduje również swoje odzwierciedlenie w orzecznictwie sądów administracyjnych. Naczelny Sąd Administracyjny wskazał[121], iż cyt.: „Wspomniane zadania publiczne, w imię których ma się odbywać przetwarzanie danych osobowych, muszą być określone prawem. Ustawa o ochronie danych osobowych nie definiuje jednak pojęcia "*zadań realizowanych dla dobra publicznego"*, ani też nie określa bliżej podmiotów wykonujących te zadania publiczne. W ocenie Naczelnego Sądu Administracyjnego chodzi tu o zadania, które zostały zlecone przez prawo temu podmiotowi, który dane przetwarza. Mogą to być zadania z zakresu bezpieczeństwa publicznego, walki z przestępczością, udzielania pomocy ofiarom klęsk żywiołowych, itd. Podmiotami wykonującymi zadania publiczne mogą zaś być organy państwowe, samorządowe, państwowe lub komunalne jednostki organizacyjne, a także podmioty wymienione w art. 3 ust. 2 ustawy o ochronie danych osobowych. Niewątpliwie do

[118] Decyzja GIODO z dnia 25 września 2015 r. DOLiS/DEC-780/15/87577,87578.
[119] Pismo GIODO z dnia 25 września 2015 r. DOLiS-440-1683/14/MKR/I/87574.
[120] M.in. Decyzja GIODO z dnia 29 stycznia 2015 r. DOLiS/DEC-50/15/6655,6668.
[121] Wyrok NSA z dnia 19 stycznia 2015 r. sygn. akt I OSK 1099/13.

takich podmiotów można zaliczyć straż gminną (miejską), która w rozumieniu art. 6 ust. 1 ustawy o strażach gminnych jest jednostką organizacyjną gminy i w oparciu o art. 10 ust. 1 tej ustawy wykonuje zadania w zakresie ochrony porządku publicznego, wynikające z ustaw i aktów prawa miejscowego. Wykonywanie czynności podejmowanych przez Straż Miejską w postępowaniu w sprawach o wykroczenia ma na celu ochronę porządku publicznego. Wobec tego bezspornym jest, że również i druga z wymienionych wyżej przesłanek została w niniejszej sprawie spełniona, skoro uzyskanie przez Straż Miejską danych osobowych abonenta telefonu komórkowego, czyli osoby podejrzanej o popełnienie wykroczenia, było konieczne do wykonania określonych prawem zadań realizowanych przez Straż Miejską dla dobra publicznego. (…) Wskazane przepisy nie tylko uprawniają, ale wręcz zobowiązują Straż Miejską do pozyskania wszelkich niezbędnych danych w celu ustalenia sprawcy wykroczenia, a następnie skierowania do sądu stosownego wniosku o ukaranie podmiotu w pełni zidentyfikowanego. (…) Odmowa udostępnienia Straży Miejskiej żądanych danych osobowych użytkownika, w sytuacji gdy jedynymi danymi, jakimi dysponowała straż był jego numer telefonu komórkowego, a Spółka [..] była jedynym dysponentem tych danych, stanowiła niewątpliwie przeszkodę w zrealizowaniu nałożonych na Straż Miejską obowiązków wynikających z przepisów prawa".

Warto wskazać również na wyrok Naczelnego Sądu Administracyjnego, który w sprawie dotyczącej przetwarzania danych osobowych przez operatora telekomunikacyjnego w sytuacji unieważnienia przez sąd cywilny umowy o świadczenie usług telekomunikacyjnych, orzekł, iż cyt.: „Według art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przetwarzanie danych jest dopuszczalne wtedy, gdy jest to niezbędne do realizacji obowiązku wynikającego z przepisów. W sytuacji, gdy stwierdzono nieważność umowy cywilnoprawnej, będącej podstawą wystawienia faktur podatku od towarów i usług, przedsiębiorca nadal może przetwarzać dane osobowe strony umowy w zakresie jej imienia, nazwiska, adresu zameldowania i numeru NIP na podstawie art. 32 § 1, art. 86 § 1 oraz art. 88 § 1 ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2015 r. poz. 613)"[122].

3.3.13. Zatrudnienie

W omawianym roku sprawozdawczym, do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **47 skarg**, w których zakwestionowano legalność działań sektorze **zatrudnienia**, tj. w procesie przetwarzania danych osobowych skarżących przez pracodawców, a w znacznej większości przez byłych pracodawców.

[122] Wyrok NSA z dnia 10 lipca 2015 r. sygn. akt I OSK 2498/13.

W jednej ze skarg Skarżący był jednocześnie pracownikiem i klientem banku. Skarżący wskazał, że w związku ze złożeniem reklamacji do ww. banku, a w następstwie również i skargi do KNF, bank jako pracodawca Skarżącego posłużył się tymi informacjami w celu złożenia wypowiedzenia Skarżącemu. Zebrany w sprawie materiał dowodowy nie pozostawiał wątpliwości, iż doszło do wykorzystania danych osobowych Skarżącego jako klienta banku, przez bank w stosunkach pracowniczych, tj. złożenia Skarżącemu wypowiedzenia umowy o pracę (co potwierdził zresztą sam bank w złożonych wyjaśnieniach). Zatem powyższe było przetwarzaniem danych osobowych Skarżącego niezgodne z pierwotnym celem ich pozyskania, tj. w celu rozpatrzenia reklamacji oraz bez zachowania warunków z art. 26 ustawy. Bank oświadczył, że podjął działania zmierzające do niedopuszczenia powtórzenia się takiej sytuacji w przyszłości. Wobec powyższego należało odmówić uwzględnienia wniosku Skarżącego[123]. Jednocześnie z uwagi, iż ww. sytuacja wzbudziła wiele wątpliwości, GIODO zdecydował się skierować zawiadomienie o podejrzeniu popełnienia przestępstwa.

3.3.14. Windykacja

W roku 2015 do organu ds. ochrony danych osobowych wpłynęło **110 skarg** dotyczących sektora **windykacji,** czyli dokładnie tyle samo, ile w roku ubiegłym. Praktycznie wszystkie skargi w przedmiocie windykacji dotyczyły zbadania legalności pozyskania i przetwarzania danych osobowych przez firmy windykacyjne.

Jak w poprzednich latach Generalny Inspektor kontynuował linię orzeczniczą dotyczącą legalności działalności firm windykacyjnych. Organ do spraw ochrony danych osobowych uznał bowiem podejmowanie działań zmierzających do zawarcia umowy sprzedaży wierzytelności jako prawnie usprawiedliwiony cel administratora danych (art. 23 ust. 1 pkt 5 ustawy w zw. z art. 23 ust. 4 pkt 2 ustawy)[124].

Ponadto wskazać należy wyrok Naczelnego Sądu Administracyjnego[125], w którym stwierdza się, iż cyt.: „przekazanie na rzecz [firmy windykacyjnej] wszystkich danych osobowych skarżącego jakimi dysponowała [Spółka będąca operatorem telekomunikacyjnym] w związku z zawartą umową, mieściło się w dyspozycji tego przepisu [art. 164 Prawa telekomunikacyjnego]. Skoro podstawą przekazania danych był przelew wierzytelności z tytułu zrealizowanej umowy o świadczenie usług telekomunikacyjnych, z czym potencjalnie wiązać się może dochodzenie tej wierzytelności w postępowaniu sądowym, to celowość przekazania tych danych mogła być oceniana z punktu widzenia potrzeb takowego

[123] Decyzja GIODO z dnia 22 grudnia 2015 r. DOLiS/DEC-973/15/107482,107486.
[124] Np. Decyzja GIODO z dnia 08 lipca 2015 r. (DOLiS/DEC-570/15/60313,60324,60333) czy też Decyzja GIODO z dnia 16 lipca 2015 r. (DOLiS/DEC-597/15/63388,63392).
[125] Wyrok NSA z dnia 10 listopada 2015 r., sygn. akt I OSK 1210/14.

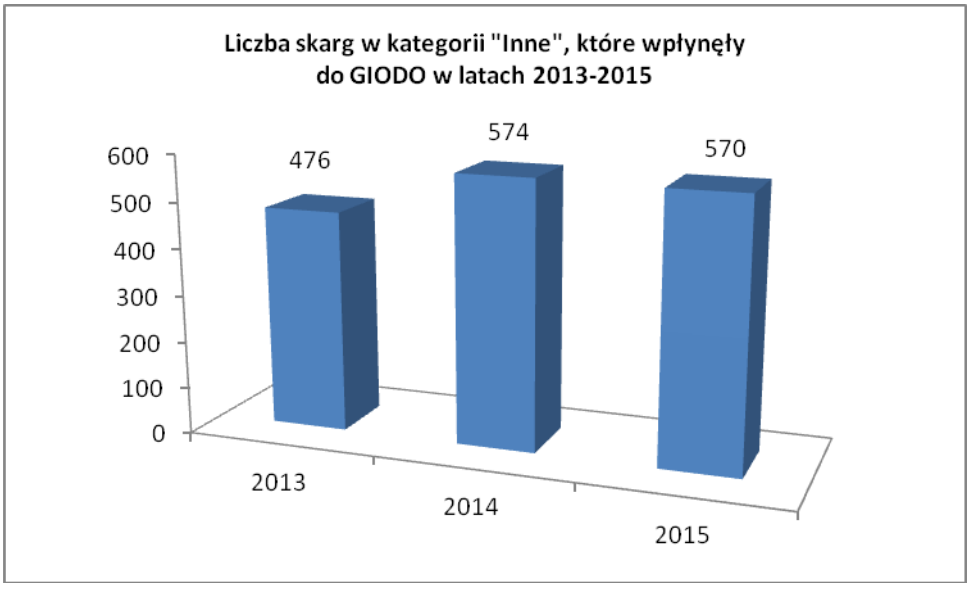
postępowania, bez ograniczenia do danych wpisanych do ewidencji działalności gospodarczej, przewidzianych w przepisie art. 7a ust. 2 ustawy z 19 listopada 1999 r. - Prawo działalności gospodarczej".

3.3.15. Inne

Wśród skarg, które Generalny Inspektor Ochrony Danych Osobowych badał w 2015 r. wyodrębnić należy te, które z racji swojego przedmiotu nie mogły być zakwalifikowane do wcześniej przedstawionych kategorii spraw. Ich liczba wyniosła **570,** co stanowi liczbę porównywalną w stosunku do roku 2014, w którym skarg tych odnotowano 574.

W tym miejscu przede wszystkim należy wskazać, że w omawianym sektorze występowały – jak w latach poprzednich - skargi zawierające zarzut nielegalnego przetwarzania danych osobowych przez proboszczów **parafii Kościoła Katolickiego** (**73 skargi** spośród ogółu 570, które wpłynęły do Biura GIODO w 2015 r.). Ponadto wskazać należy, iż w 2015 r. GIODO wydał łącznie 120 decyzji w sprawach dotyczących Kościoła Katolickiego, z czego 73 razy nakazywał przywrócenie stanu zgodnego z prawem, 7 razy umarzał postępowanie, w 5 przypadkach odmawiał uwzględniania wniosku. Ponadto w 35 sprawach utrzymał w mocy zaskarżoną decyzję po złożonym wniosku o ponowne rozpatrzenie sprawy zakończonej decyzją administracyjną.

Podkreślenia wymaga, iż m.in. wskutek niejednolitości orzecznictwa sądów administracyjnych, będącego wynikiem skarg stron postępowania na decyzje GIODO (zarówno Skarżących, jak i proboszczów parafii rzymskokatolickich), Generalny Inspektor Ochrony Danych Osobowych obciążany jest wciąż dodatkowymi obowiązkami, co powoduje niejednokrotnie utrudnienia w sprawnym działaniu organu. W szczególności wskazać należy, iż początkowo w ocenie NSA Generalny Inspektor powinien ustalać kwestie uaktualnienia danych osobowych apostatów na gruncie przepisów powszechnie obowiązujących, natomiast według aktualnego stanowiska NSA Generalny Inspektor winien powyższe sprawy rozstrzygać zgodnie z przepisami wewnętrznymi kościoła.



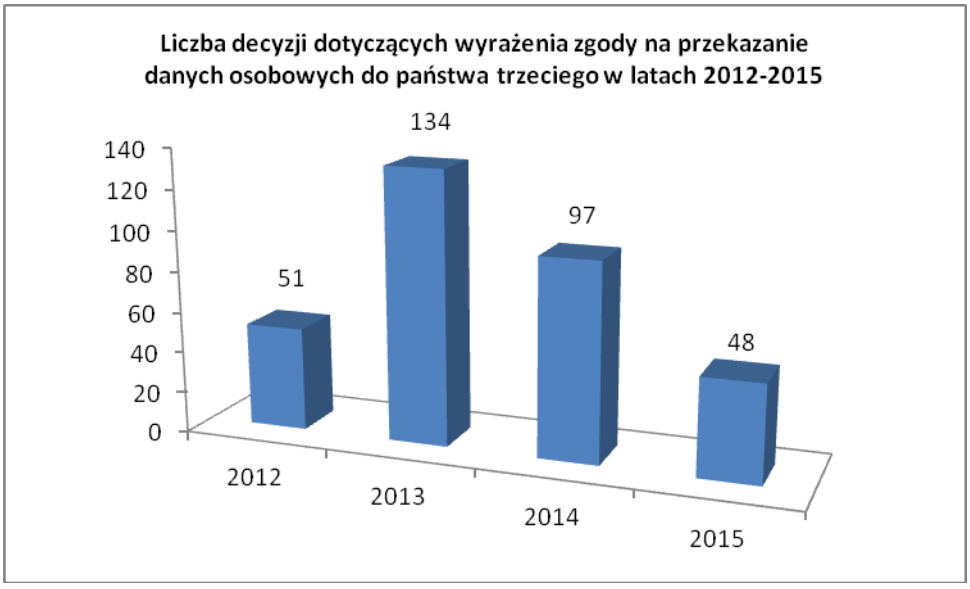
Wykres 16: ***Zestawienie porównawcze liczby skarg z sektora „Inne", które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w latach 2013–2015.***

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 Ochrony Danych Osobowych wydał w 2015 r. 48 decyzji administracyjnych dotyczących przekazania danych osobowych do państw trzecich[126]**.** Niemniej należy zaznaczyć, że część decyzji została wydana w postępowaniach administracyjnych, które zostały zainicjowane w poprzednich latach.

[126] 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 2012-2015.***

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 (WRK)**. Nowe przepisy wprowadziły w polskim porządku prawnym instytucję wiążących reguł korporacyjnych oraz określiły tryb ich zatwierdzenia przez GIODO.

Standardowe klauzule umowne zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 95/45/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 można stosować w umowach z podmiotami z państw trzecich. Wiążące reguły korporacyjne natomiast dotyczą podmiotów należących do tej samej grupy przedsiębiorców (tej samej grupy kapitałowej). Wiążące reguły korporacyjne mogą być stosowane po ich zatwierdzeniu przez Generalnego Inspektora (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, Generalny Inspektor może je uwzględnić

W związku z powyższym przeważająca większość prowadzonych przez Generalnego Inspektora postępowań administracyjnych (39 decyzji) została zakończona wydaniem decyzji umarzającej postępowanie z uwagi na zastosowanie przez administratora standardowych klauzul umownych ochrony danych osobowych. Generalny Inspektor także wydał 8 decyzji zatwierdzających WRK. Należy wskazać, że we wszystkich postępowaniach dotyczących WRK, Generalny Inspektor uwzględnił rozstrzygnięcia organów ochrony danych osobowych z innych państw należących do Europejskiego Obszaru Gospodarczego, które uprzednio zaakceptowały dane WRK. Dodatkowo Generalny Inspektor wydał jedną decyzję wyrażające zgodę na przekazanie danych osobowych do państwa trzeciego na podstawie umowy, która nie posiadała przymiotu standardowości.

Warto podkreślić, że 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.

Na szczególną uwagę zasługuje wydarzenie, wokół którego skupiona była uwaga organów ochrony danych osobowych w 2015 r. – mianowicie wyroku w sprawie Schrems.

W dniu 6 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej wydał orzeczenie w sprawie w sprawie C-362-14, Maximilian Schrems przeciwko Data Protection Commissioner (dalej jako sprawa Schrems), w którym stwierdził nieważność decyzji Komisji Europejskiej z dnia 26 lipca 2000 r. w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach "bezpiecznej przystani" przez Stany Zjednoczone, która pozwalała na przekazywanie danych osobowych przez administratorów danych, posiadających siedzibę w UE, do podmiotów amerykańskich, które przystąpiły do programu „bezpiecznej przystani” (ang. Safe Harbour) i zobowiązały się tym samym do przestrzegania

odpowiednich standardów ochrony danych osobowych. Wyrok ten ma ogromne znaczenie praktyczne, gdyż od chwili jego wydania administratorzy danych, z siedzibą w UE (w tym w Polsce) nie mogą przekazywać danych do Stanów Zjednoczonych Ameryki na podstawie unieważnionej decyzji Komisji Europejskiej. W konsekwencji, aktualnie uczestnictwo odbiorcy danych ze Stanów Zjednoczonych Ameryki w programie „bezpiecznej przystani" nie pozwala już na uznanie, że przekazanie do niego danych jest równoznaczne z przekazaniem danych do państwa trzeciego, które zapewnia odpowiedni poziom ochrony danych osobowych, o którym mowa w art. 47 ust 1 i 1a ustawy o ochronie danych osobowych**.** Z tego względu w aktualnym stanie prawnym przekazanie danych osobowych do Stanów Zjednoczonych Ameryki wymaga spełnienia jednej z przesłanek określonych w art. 47 albo 48 ustawy o ochronie danych osobowych. W szczególności nadal możliwe jest stosowanie w odniesieniu do takich transferów standardowych klauzul umownych oraz zatwierdzonych przez Generalnego Inspektora wiążących reguł korporacyjnych.

W 2016 r. na poziomie UE będą trwały prace nad wydaniem nowej decyzji Komisji Europejskiej w sprawie adekwatności ochrony danych osobowych w Stanach Zjednoczonych Ameryki. W szczególności krajowe organy ochrony danych osobowych skupione w ramach Grupy Roboczej Art. 29 będą szczegółowo analizować zaproponowane rozwiązania pod względem ich zgodności z zasadami ochrony danych osobowych w Unii Europejskiej, ze szczególnym uwzględnieniem praw podstawowych obywateli UE.

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

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.[127]

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 2015 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęły **93 zawiadomienia o naruszeniu danych osobowych.**

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

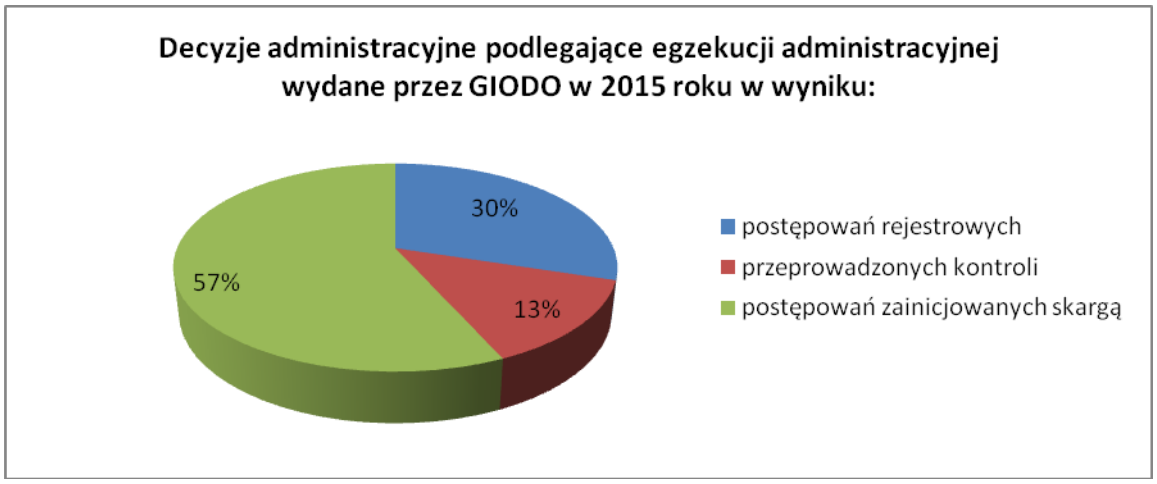
W celu zapewnienia wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych, Generalny Inspektor - na podstawie art. 12 pkt 3 ustawy o ochronie danych osobowych - uprawniony jest do stosowania środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2014 r. poz. 1619 z późn. zm.). W celu realizacji tego zadania, Generalny Inspektor Ochrony Danych Osobowych 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 zawierała postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlegał egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek do wykonania nakładany na stronę (zobowiązanego) może polegać na usunięciu uchybień, uzupełnieniu, uaktualnieniu, sprostowaniu, udostępnieniu lub nieudostępnieniu danych osobowych, zastosowaniu dodatkowych środków zabezpieczających zgromadzone dane

[127] 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.

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 2015 r. Generalny Inspektor wydał **97 decyzji administracyjnych** zawierających nałożony na strony nakaz (obowiązek) do wykonania i **podlegających egzekucji administracyjnej**. Spośród decyzji wydanych w 2015 r. **29** (46 %) dotyczyło postępowań rejestrowych, **13** (13 %) zostało wydanych w związku z przeprowadzonymi kontrolami, **55** (57 %) wydano na skutek postępowania zainicjowanego skargą.

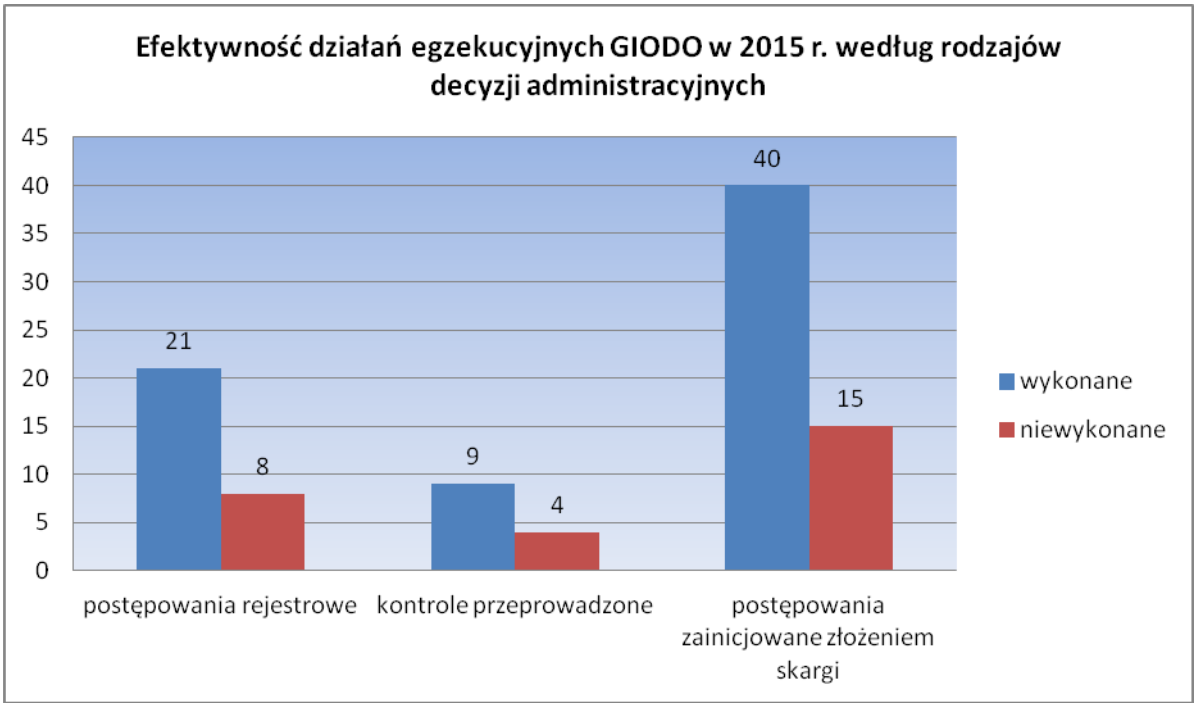


Wykres 18: ***Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji, wydanych przez GIODO w 2015 r.***

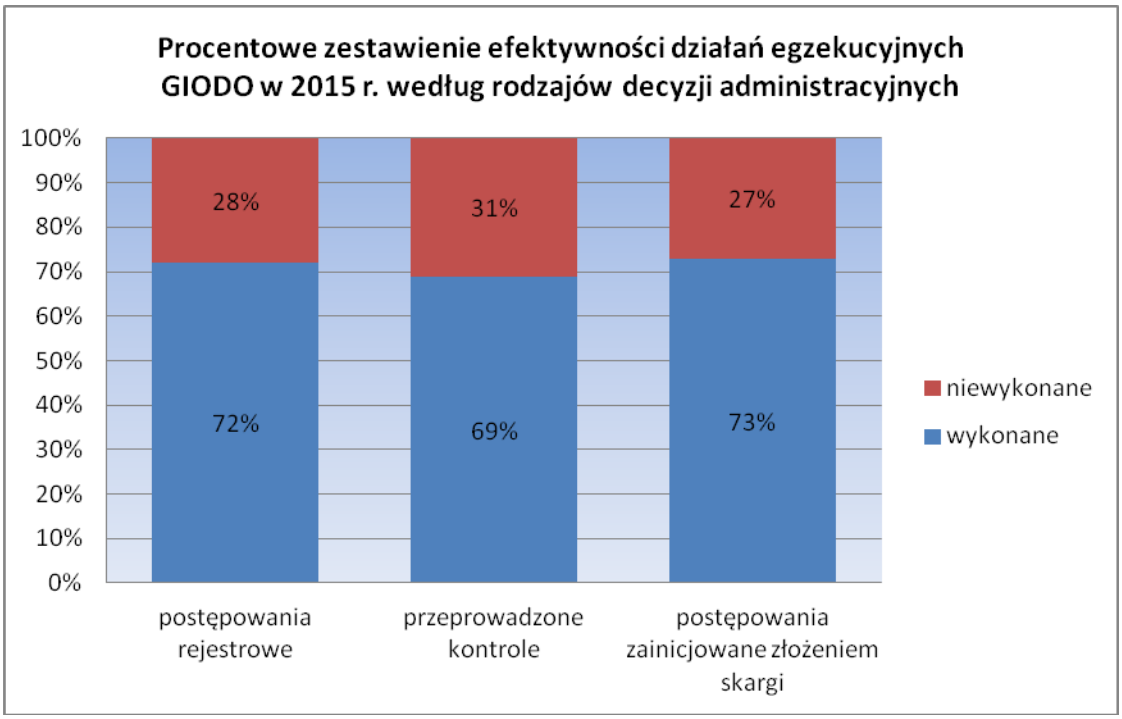
Efektywność prowadzonych w 2015 r. przez Generalnego Inspektora działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków, przedstawia się następująco: spośród 97 decyzji administracyjnych **wykonanych zostało przez zobowiązanych 70 decyzji**, 27 decyzji na koniec 2015 r. pozostało niewykonanych. Decyzje te objęte są działaniami egzekucyjnymi w 2016 r. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań Generalnego Inspektora Ochrony Danych Osobowych oraz przeprowadzonych kontroli sprawdzających. W 22 przypadkach wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia zobowiązani w 11 przypadkach wykonali w całości decyzję administracyjną GIODO.

Wobec 2 zobowiązanych prowadzone było postępowanie egzekucyjne wszczęte jeszcze w 2014 r. na podstawie wystawionych tytułów wykonawczych, z zastosowaniem środka egzekucyjnego w postaci ponownego w 2015 r. nałożenia grzywny w celu przymuszenia (w obu przypadkach wysokość ponownej grzywny wyniosła 40.000 zł). Poprzednio wysokość grzywny w celu przymuszenia w obu przypadkach wyniosła 25.000 zł. W stosunku do tych podmiotów postępowanie egzekwujące zostało w 2015 r. zakończone w związku z wykonaniem przez zobowiązanego w całości obowiązku zawartego w tytule wykonawczym.

Spośród decyzji wydanych w 2015 r. i wykonanych przez zobowiązanych w 2015 r. **21 dotyczyło postępowań rejestrowych, 9 zostało wydanych w związku z przeprowadzonymi kontrolami, 40 wydano na skutek postępowania zainicjowanego skargą.** Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w 2015 r. wynosił **72%.** W odniesieniu do postępowań rejestrowych efektywność egzekucji wynosiła **72%**, wobec decyzji wydanych w związku z przeprowadzonymi kontrolami - **69%**, natomiast w stosunku do decyzji wydanych na skutek postępowań zainicjowanych skargą - **73%**.



Wykres 19: ***Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2015 r.***

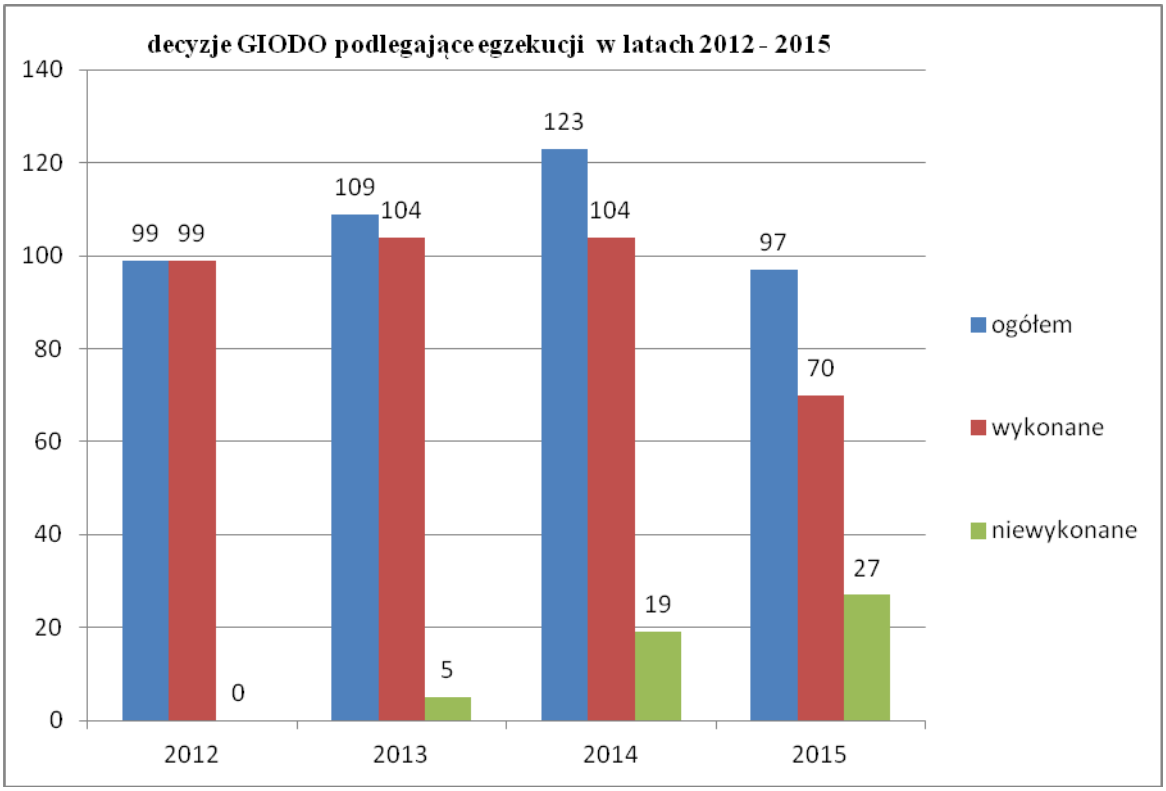


Wykres 20: ***Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2015 r.***

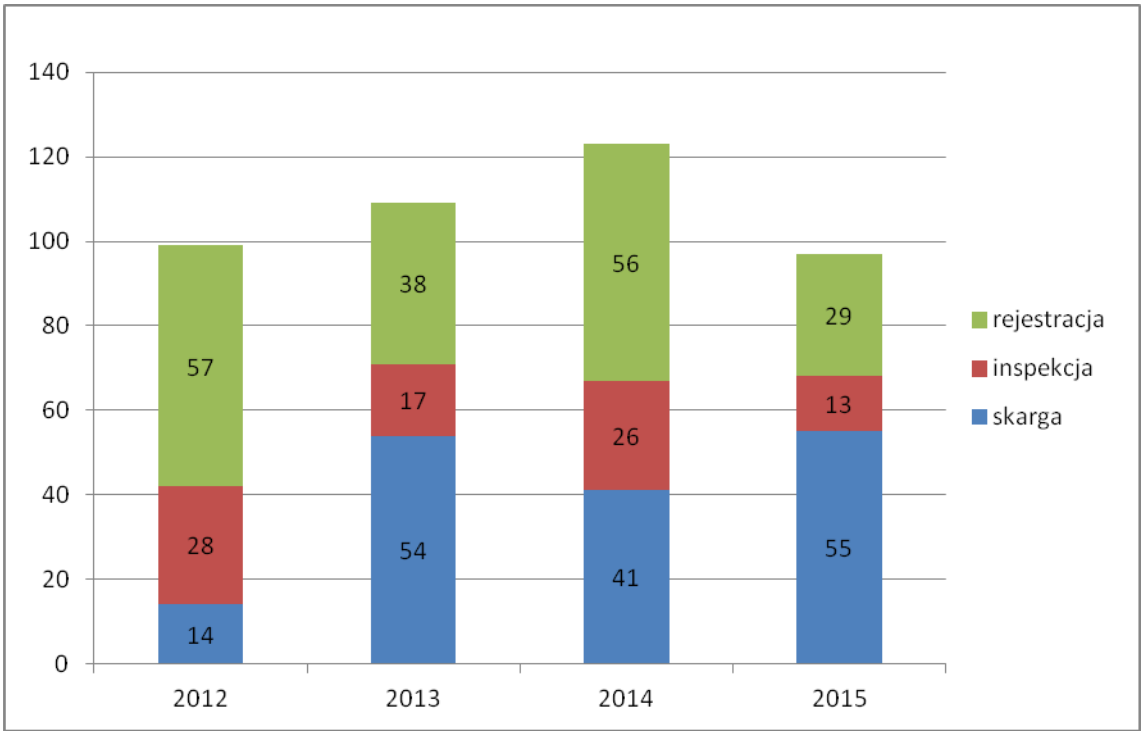
Można zaobserwować zmianę trendu w odniesieniu do wydawanych przez GIODO decyzji administracyjnych podlegających egzekucji administracyjnej. W 2013 r. decyzji było 109. W 2014 r. wpłynęło 123 decyzje, co stanowiło wzrost o 13% w stosunku do roku poprzedniego. Natomiast w 2015 r. wpłynęło jedynie 97 decyzji administracyjnych, co stanowi spadek o 21% w stosunku do roku poprzedniego.

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w latach 2012-2015 przedstawia się następująco: spośród decyzji GIODO objętych egzekucją administracyjną w **2012 r**. efektywność wynosiła **100%**, natomiast w zakresie decyzji GIODO objętych egzekucją administracyjną w **2013 r.** efektywność utrzymywała się na poziomie **95%.** W odniesieniu do postępowań egzekucyjnych prowadzonych w **2014 r.** efektywność egzekucji wynosiła **84%**, natomiast w odniesieniu do postępowań egzekucyjnych prowadzonych w **2015 r. - 72%.** Niższy wskaźnik efektywności w 2015 r. wynikał z faktu, iż wobec tych decyzji działania egzekucyjne zostały rozpoczęte, zobowiązani sukcesywnie wykonywali

nakazy zawarte w decyzjach oraz byli w trakcie składania informacji o wykonaniu decyzji do Generalnego Inspektora Ochrony Danych Osobowych.



Wykres 21: ***Zestawienie decyzji GIODO podlegających egzekucji administracyjnej i efektywność podejmowanych działań egzekucyjnych w latach 2012 – 2015.***



Wykres 22: ***Zestawienie decyzji GIODO podlegających egzekucji administracyjnej ze względu na źródło pochodzenia nakazu w latach 2012 – 2015.***

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

Na mocy art. 9 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r. poz. 1662), który wszedł w życie w dniu 1 stycznia 2015 r., doszło do znaczącej zmiany przepisów ustawy o ochronie danych zwanej dalej również „ustawą". Zgodnie z nowym brzmieniem przepisu art. 12 pkt 4 ustawy, do zadań Generalnego Inspektora należy prowadzenie rejestru zbiorów danych oraz rejestru administratorów bezpieczeństwa informacji, a także udzielanie informacji o zarejestrowanych zbiorach i zarejestrowanych administratorach bezpieczeństwa informacji, zaś na podstawie art. 46c ustawy, Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji. Zadania te realizowane są przez Departament Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych. W znowelizowanej ustawie rozszerzeniu uległ również katalog wyłączeń z obowiązku zgłoszenia zbioru danych do rejestracji. Zgodnie z art. 43 ust. 1 pkt 12 ustawy, z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów

zawierających dane, o których mowa w art. 27 ust. 1 ustawy tj. dane szczególnie chronione. Należy w tym miejscu podkreślić, że zwolnienie to dotyczy wszystkich administratorów danych. Ponadto od 1 stycznia 2015 r., zgodnie z art. 43 ust. 1a ustawy, obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1 ustawy, nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. To zwolnienie koreluje z obowiązkami administratora danych. Jednym z zadań należących do administratorów bezpieczeństwa informacji jest bowiem prowadzenie rejestru zbiorów danych osobowych przetwarzanych przez administratora danych (art. 36a ust. 2 pkt 2 ustawy). Rejestr jest prowadzony u administratora danych i obejmuje wszystkie zbiory danych prowadzone przez tego administratora (z wyjątkiem zbiorów danych wyłączonych dotychczas z obowiązku zgłoszenia do rejestracji GIODO na podstawie w art. 43 ust. 1 ustawy). Administrator bezpieczeństwa informacji powinien zatem ująć w swoim rejestrze również zbiory uprzednio - tj. przed 1 stycznia 2015 r. - zgłoszone do Generalnego Inspektora (w tym zbiory zawierające dane wrażliwe).

Zakładano, że nowe wyjątki od zasady zgłaszania zbiorów danych do rejestracji wpłyną na zmniejszenie liczby zgłoszeń zbiorów danych nadsyłanych do Generalnego Inspektora. Nie do końca zmiana ustawy przyniosła spodziewane skutki, o czym będzie mowa w dalszej części sprawozdania, ale z pewnością nowy stan prawny zmodyfikował od 1 stycznia 2015 r. funkcję informacyjną rejestru zbiorów danych osobowych prowadzonego przez Generalnego Inspektora. Przed nowelizacją ustawy jawny i ogólnopolski rejestr zbiorów danych osobowych prowadzony przez Generalnego Inspektora Ochrony Danych Osobowych zapewniał wszystkim zainteresowanym dostęp do informacji o administratorach danych i prowadzonych przez nich zbiorach danych osobowych. Obecnie osoba zainteresowana tym, w jaki sposób i przez jakie podmioty przetwarzane są jej dane osobowe, powinna w pierwszej kolejności dokonać sprawdzenia w prowadzonym przez Generalnego Inspektora rejestrze administratorów bezpieczeństwa informacji, czy interesujący ją administrator danych powołał i zgłosił do rejestracji administratora bezpieczeństwa informacji. W przypadku odpowiedzi negatywnej, informacje o zbiorach danych zgłoszonych przez administratora danych będą dostępne wyłącznie w ogólnokrajowym, jawnym rejestrze Generalnego Inspektora. Jeśli administrator danych powołał administratora bezpieczeństwa informacji, wówczas informacji o zbiorach należy poszukiwać przede wszystkim w jawnym rejestrze zbiorów danych prowadzonym przez właściwego administratora bezpieczeństwa informacji. Od 1 stycznia

2015 r. informacje umieszczone w jawnym rejestrze zbiorów prowadzonym przez administratora bezpieczeństwa informacji nie muszą być aktualizowane w rejestrze Generalnego Inspektora, z wyjątkiem informacji dotyczących zbiorów zawierających dane szczególnie chronione.

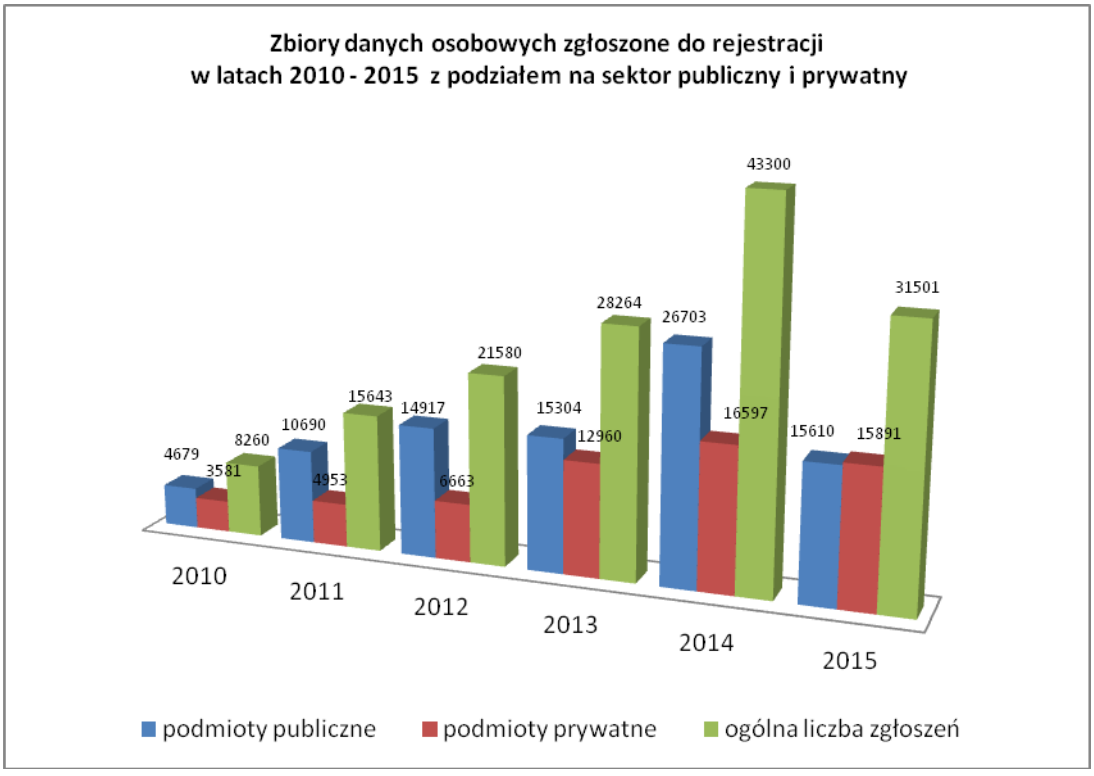
Należy podkreślić, że ustawodawca uznał jednak, iż kontrola wstępna dotycząca zwłaszcza zbiorów zawierających dane wrażliwe w dalszym ciągu powinna być wykonywana przez Generalnego Inspektora Ochrony Danych Osobowych. Na podstawie przesłanego przez administratora danych zgłoszenia zbioru danych, Generalny Inspektor ocenia przestrzeganie przez administratora danych zasad przetwarzania danych osobowych, w tym sprawdza, czy istnieje podstawa prawna do przetwarzania danych osobowych, czy pozyskiwane są wyłącznie dane adekwatne do celu przetwarzania, a także czy spełnione są podstawowe wymogi w zakresie zabezpieczenia przetwarzanych danych osobowych. Odmawiając rejestracji zbioru danych, w drodze decyzji wydanej na podstawie art. 44 ustawy o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych nakazuje ograniczenie przetwarzania wszystkich albo niektórych kategorii danych wyłącznie do ich przechowywania do czasu zarejestrowania zbioru po jego ponownym zgłoszeniu oraz zastosowanie innych środków, o których mowa w art. 18 ust. 1 ustawy, tj. w szczególności: zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe lub usunięcie danych osobowych (w przypadku gdy pozyskiwane dane są nieadekwatne do celu ich przetwarzania). Ponowne zgłoszenie zbioru do rejestracji może nastąpić po usunięciu wad, które były powodem odmowy rejestracji tego zbioru, zaś przetwarzanie danych może rozpocząć się dopiero po zarejestrowaniu zbioru. Zatem decyzja Generalnego Inspektora usuwa naruszenia w procesie przetwarzania danych, a ponadto pozwala na podjęcie przetwarzania dopiero po zaniechaniu naruszania prawa i sprawdzeniu tego przez Generalnego Inspektora (co do zasady na podstawie oświadczenia administratora danych).

Informacje uzyskane w toku postępowania rejestracyjnego stanowią także dla organu ds. ochrony danych osobowych podstawowe źródło wiedzy na temat administratorów danych, prowadzonych przez nich zbiorów danych oraz warunków przetwarzania danych w tych zbiorach. Posiadanie tych informacji pozwala zdefiniować problemy występujące w procesie przetwarzania danych w określonych obszarach i podjąć działania zmierzające do przywrócenia stanu zgodnego z prawem. Informacje z rejestru często są wykorzystywane przy planowaniu kontroli u danego administratora danych, czy kontroli branżowych.

Należy zwrócić uwagę, że w przepisach nowego rozporządzenia ogólnego o ochronie danych osobowych, rejestracja zbiorów danych nie będzie już wymagana, przewidywana jest natomiast ocena skutków przetwarzania pod kątem ochrony danych dokonywana przez administratora danych i uprzednie konsultacje z organem nadzorczym. Organ nadzorczy ma ustanawiać i podawać do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi oceny w zakresie ochrony danych (może to być też wykaz negatywny, zawierający wyłączenia w zakresie dokonywania tej oceny). Jeśli ocena skutków dokonana przez administratora danych wykaże, że przetwarzanie danych niosłoby duże zagrożenie, przed rozpoczęciem przetwarzania danych administrator miałby obowiązek skonsultowania się z organem nadzorczym. Takie konsultacje to niejako kontrola wstępna dokonywana przez organ nadzorczy. Jest ona dość sformalizowana, administrator danych przekazuje bowiem organowi nadzoru określone w rozporządzeniu informacje dotyczące zamierzonego przetwarzania, organ nadzorczy może zaś żądać wszelkich innych informacji Niezależnie od tego prawo państw członkowskich może wymagać, aby administratorzy danych konsultowali się z organem nadzorczym i uzyskiwali jego uprzednie zezwolenie dotyczące przetwarzania danych do celów wykonywania zadania realizowanego w interesie publicznym, w tym w związku z ochroną socjalną zdrowiem publicznym. Oczywiście byłoby to regulowane odrębnym aktem prawnym lub odpowiednie przepisy powinny być wprowadzone do właściwych ustaw kompetencyjnych. Ciekawym zagadnieniem jest też forma „zezwalania" na przetwarzanie, o którym mowa w art. 36 ust. 5 projektu (czy też braku takiego zezwolenia) od organu nadzoru. Czy miałby zastosowanie Kodeks postępowania administracyjnego, ze wszystkimi tego konsekwencjami (dwuinstancyjność, skarga do sądu), czy też należałoby określić odrębny tryb postępowania organu nadzoru – co jeszcze wymaga rozstrzygnięcia. Natomiast warto skorzystać z dotychczasowego dorobku i doświadczeń GIODO dotyczących przeprowadzania kontroli wstępnej. Postępowania prowadzone w związku z rozpatrywaniem zgłoszeń zbiorów danych do rejestracji GIODO mają bowiem także istotny walor edukacyjny w stosunku do administratorów danych i podmiotów przetwarzających dane osobowe. Obowiązek zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych oraz świadomość skutków ewentualnej odmowy rejestracji zbioru, 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 2015 r. wysłano do administratorów danych blisko 2 tysiące pism zawierających tego rodzaju informacje. Skutek edukacyjny ma wpływ na prawidłowe prowadzenie również innych zbiorów tworzonych przez danego administratora danych.

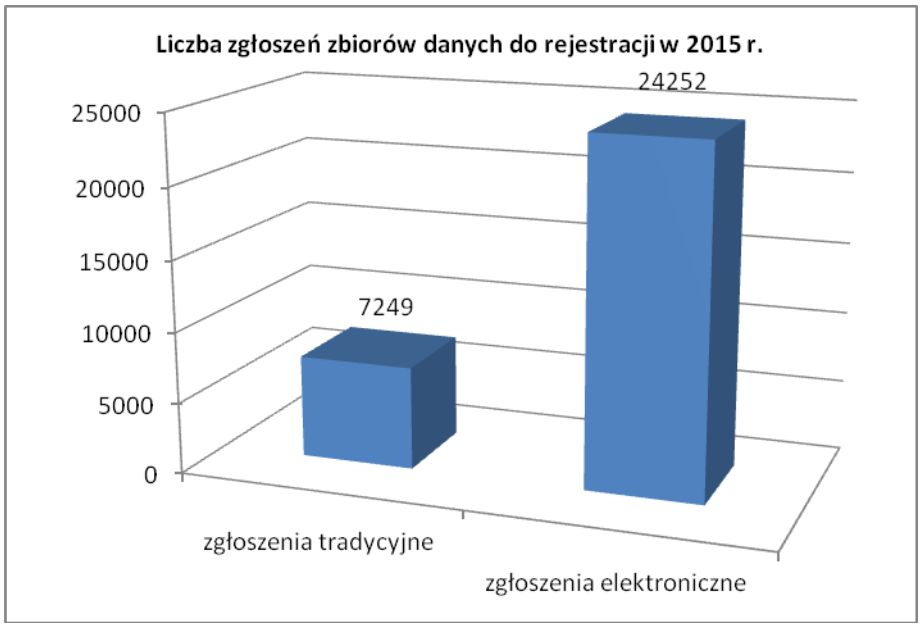
W 2015 roku, administratorzy danych, wypełniając obowiązek określony w art. 40 ustawy o ochronie danych osobowych[128], **zgłosili do rejestracji** Generalnemu Inspektorowi Ochrony Danych Osobowych **31501 zbiorów danych osobowych**, z czego podmioty z sektora administracji publicznej zgłosiły **15610 zbiorów**, co stanowiło 49 % ogólnej liczby zgłoszeń dokonanych w tym okresie, zaś podmioty z sektora prywatnego - **15891 zbiorów**, co stanowiło 51% ogólnej liczby zgłoszonych zbiorów.



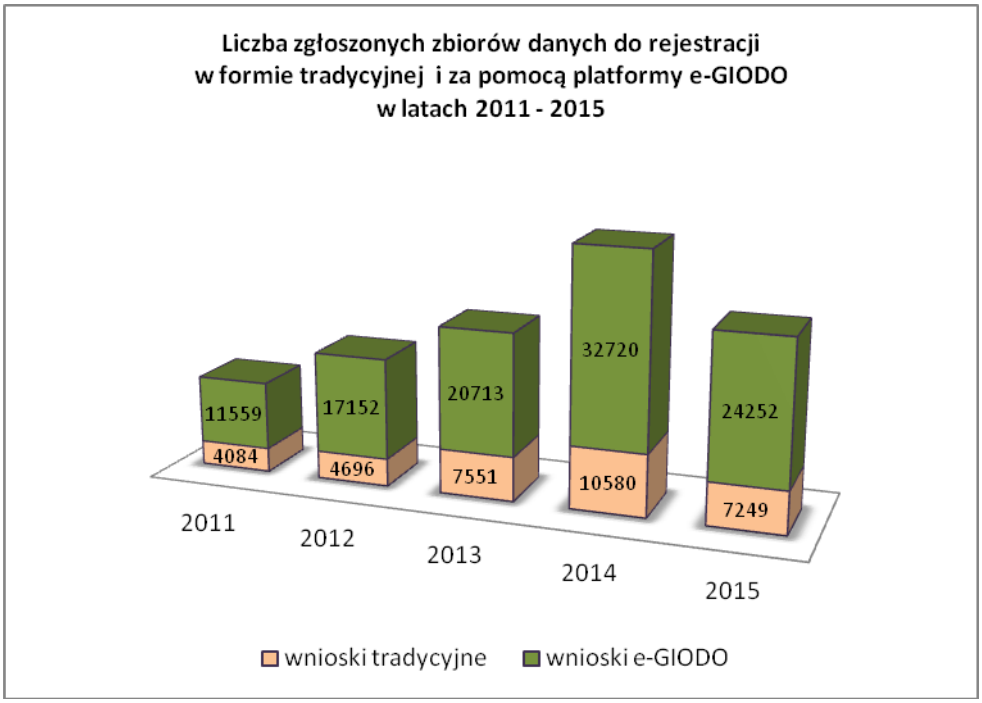
Wykres 23: ***Liczbowe zestawienie zbiorów danych osobowych zgłoszonych do rejestracji przez podmioty publiczne i prywatne w latach 2010 - 2015.***

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

W 2015 roku **przy użyciu programu wspomagającego (eGIODO)**, udostępnionego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych, **zgłoszono do rejestracji 24252 zbiory danych.** Zgłoszenia dokonane drogą elektroniczną stanowiły 77 % wszystkich zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2015 roku. Jest to wynik porównywalny do poprzednich okresów sprawozdawczych (2014 – 75%, 2013 – 73 %, 2012 – 78 %).



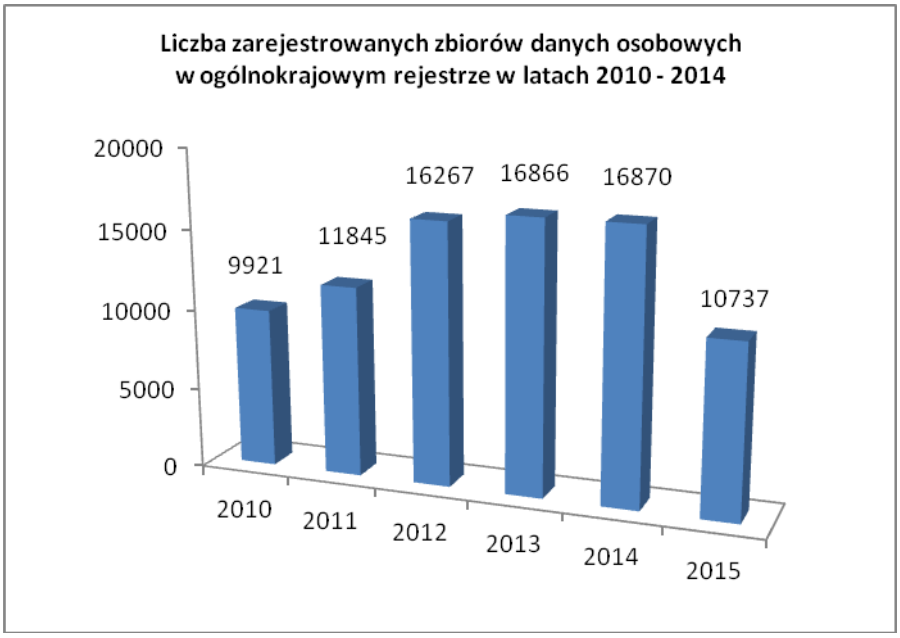
Wykres 24: ***Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonanych w 2015 r. w formie tradycyjnej i elektronicznej.***



Wykres 25: ***Zestawienie porównawcze zgłoszeń zbiorów danych do rejestracji dokonywanych w latach 2011 - 2015 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 **12728.** 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 10737 zbiorów danych.**



Wykres 26: ***Zestawienie porównawcze zarejestrowanych zbiorów danych osobowych w ogólnokrajowym rejestrze w latach 2010 - 2015.***

Stosunkowo często informacje zawarte w zgłoszeniu nie pozwalały na zakończenie sprawy bez przeprowadzenia postępowania wyjaśniającego. W 2015 roku, w toku postępowań rejestracyjnych do wnioskodawców **skierowano 893 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 toku postępowania prowadzonego w związku ze zgłoszeniem zbioru do rejestracji 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 i 1a ustawy[129].

[129] W roku 2015 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

W 2015 roku wysłano do wnioskodawców **352 pisma informujące o braku obowiązku zgłoszenia do rejestracji zbioru**, wynikającym z przesłanek określonych w art. 43 ust. 1 i 1a ustawy oraz **439 pism informujących o braku podstaw do dokonania wpisów w rejestrze z innych przyczyn** (dotyczyły one 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). **Należy podkreślić, że mimo wejścia w życie nowelizacji, w roku 2015 wpłynęło więcej zgłoszeń zbiorów danych do rejestracji niż w roku 2014.** Co więcej, prawdopodobnie w związku z brakiem *vacatio legis* dla nowych przepisów, administratorzy danych często nie uwzględniali nowych wyłączeń z obowiązku rejestracji zbiorów danych i zgłaszali do rejestracji zbiory danych osobowych niepodlegające zgłoszeniu. Należało ich zatem poinformować o nowych przepisach, co niewątpliwie komplikowało bieżące rozpatrywanie prawidłowych zgłoszeń.

W wielu przypadkach przesłane zgłoszenia nie spełniały wymogów formalnych przewidzianych w ustawie z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23). W konsekwencji w 2015 roku skierowano do wnioskodawców, na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego, **690 wezwań do uzupełnienia w zgłoszeniu braków formalnych**.

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

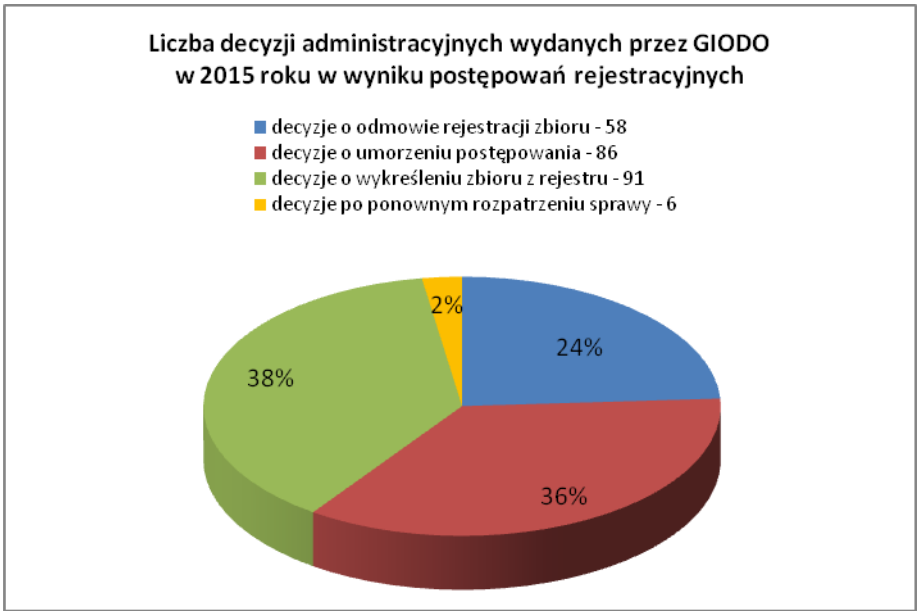
---

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) przewarzanych 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.

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 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.

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

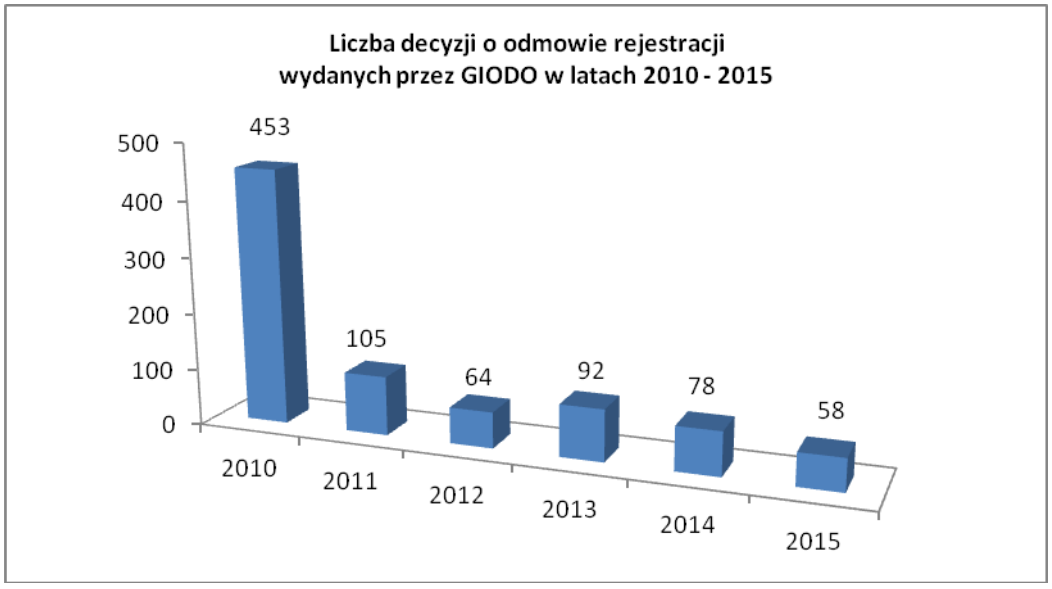
W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał ogółem **241 decyzji administracyjnych w związku z postępowaniem rejestracyjnym**. Spośród nich, **58 decyzji dotyczyło odmowy rejestracji zbioru danych, 86 – umorzenia postępowania, 6 – po ponownym rozpatrzeniu sprawy, zaś 91 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 2015 r.***

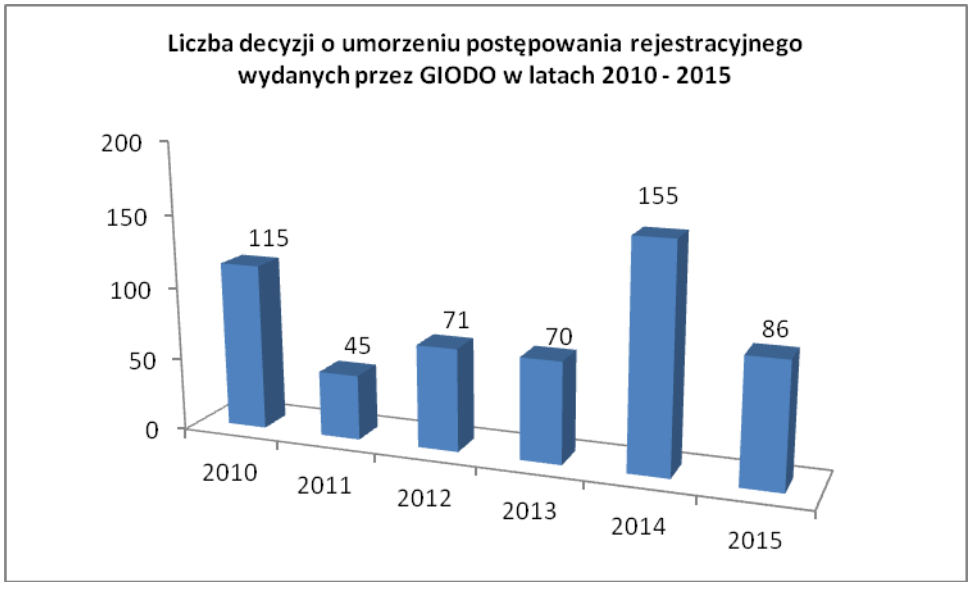
W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **58 decyzji o odmowie rejestracji zbioru danych.** Najczęściej decyzje te nakazywały usunięcie danych nieadekwatnych do celu przetwarzania. W związku z tym były bardzo dolegliwe dla administratorów danych.

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 GIODO.



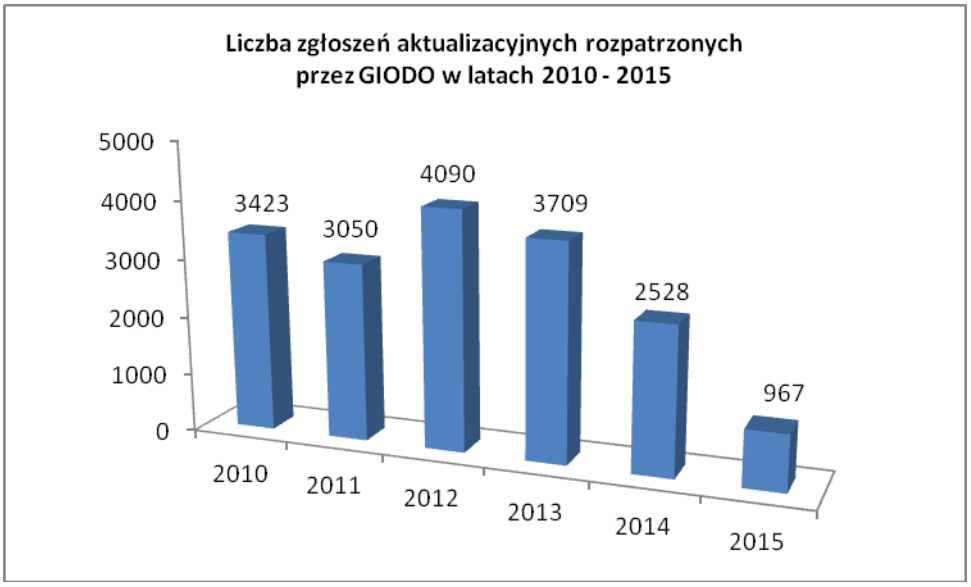
Wykres 28: ***Liczbowe zestawienie decyzji o odmowie rejestracji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010 – 2015.***

Zdarzało się, że w toku postępowania prowadzonego w związku ze zgłoszeniem zbioru danych do rejestracji wnioskodawca cofał zgłoszenie, np. informując, że zrezygnował z utworzenia zbioru danych osobowych. W takich sytuacjach postępowanie rejestracyjne stawało się bezprzedmiotowe i konieczne było wydanie decyzji o jego umorzeniu. **W 2015 roku wydanych zostało 86 decyzji o umorzeniu postępowania rejestracyjnego.**



Wykres 29: ***Zestawienie porównawcze liczby decyzji o umorzeniu postępowania rejestracyjnego wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010 - 2015.***

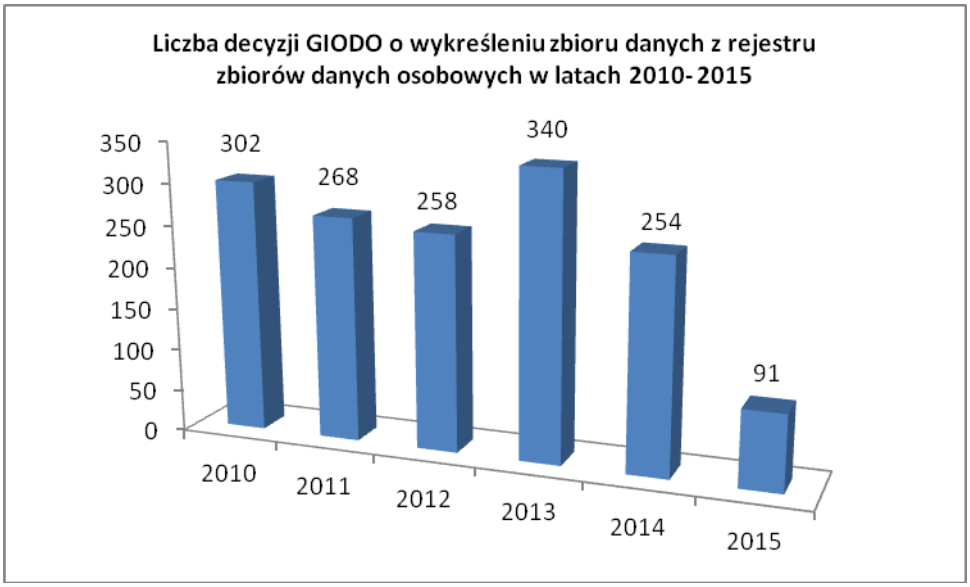
Zadania Departamentu Rejestracji Zbiorów Danych Osobowych związane z prowadzeniem rejestru zbiorów danych osobowych obejmują również rozpatrywanie zgłoszeń aktualizacyjnych, tj. zgłoszeń zmian informacji zawartych w zgłoszeniu rejestracyjnym[130] oraz prowadzenie postępowań w sprawie wykreślenia z rejestru zbiorów danych osobowych. Instytucje te dają możliwość porządkowania rejestru, zgodnie ze zmieniającymi się okolicznościami przetwarzania danych. W 2015 roku **rozpatrzonych zostało 967 zgłoszeń aktualizacyjnych** dokonanych przez administratorów danych na podstawie art. 42 ust. 2 ustawy.



Wykres 30: ***Zestawienie porównawcze liczby zgłoszeń aktualizacyjnych rozpatrzonych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010 – 2015.***

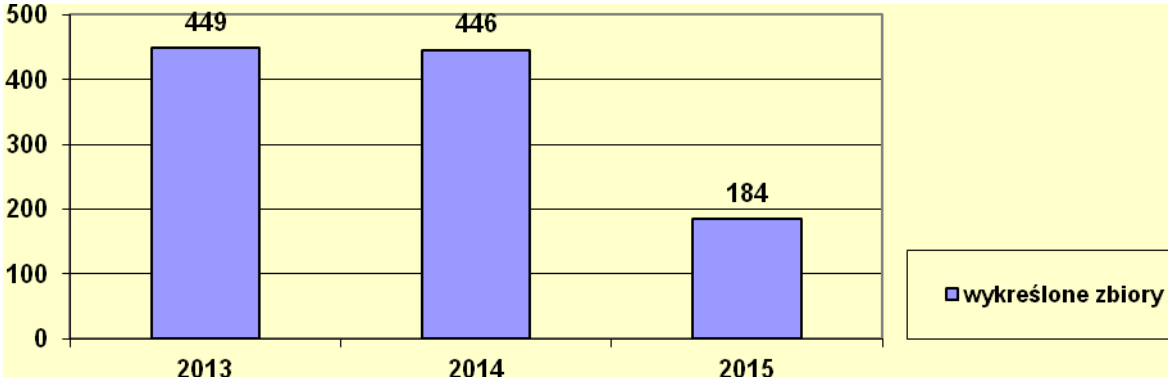
Ponadto Generalny Inspektor Ochrony Danych Osobowych wydał **91 decyzji o wykreśleniu zbioru** danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych z powodu zaprzestania przetwarzania danych w zbiorze.

[130] 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 31: ***Zestawienie porównawcze liczby decyzji o wykreśleniu zbioru z rejestru zbiorów danych osobowych w latach 2010 - 2015.***

Należy przy tym zaznaczyć, że 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 2015 roku wykreślono z rejestru 184 zbiory** danych osobowych.



Wykres 32: ***Zestawienie porównawcze liczby zbiorów wykreślonych z rejestru zbiorów danych osobowych w latach 2013 - 2015.***

W ramach wykonywania zadania polegającego na informowaniu o zarejestrowanych zbiorach, Generalny Inspektor Ochrony Danych Osobowych wydał w omawianym okresie **1.977 zaświadczeń o zarejestrowaniu zbioru danych.** W przypadku zarejestrowania zbioru danych, w którym przetwarzane były dane osobowe szczególnie chronione określone w art. 27 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wydawał zaświadczenie z urzędu, niezwłocznie po dokonaniu rejestracji takiego zbioru[131]. Administrator danych może także wystąpić z wnioskiem do Generalnego Inspektora Ochrony Danych Osobowych o wydanie zaświadczenia o zarejestrowaniu zbioru[132].

7. Rejestr zgłoszeń powołania administratora bezpieczeństwa informacji

Od dnia 1 stycznia 2015 r. Departament Rejestracji Zbiorów Danych Osobowych realizuje nowe zadania Generalnego Inspektora Ochrony Danych Osobowych związane z prowadzeniem **ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji** (art. 12 pkt 4 oraz art. 46c ustawy o ochronie danych osobowych). Ustawa o ochronie danych osobowych, znowelizowana ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r. poz. 1662), przewiduje uprawnienie administratora danych do powołania administratora bezpieczeństwa informacji. Jeżeli administrator skorzysta z tego uprawnienia, zgodnie z art. 46b ust. 1 ustawy, ma 30 dni od dnia powołania administratora bezpieczeństwa informacji na zgłoszenie tego faktu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Ponadto zgodnie z przepisami przejściowymi administrator danych, który wyznaczył administratora bezpieczeństwa informacji przed dniem 1 stycznia 2015 r. zgodnie z art. 35 ustawy o ułatwieniu wykonywania działalności gospodarczej, mógł zgłosić go do rejestru administratorów bezpieczeństwa informacji do dnia 30 czerwca 2015 r.

Art. 46b ust. 2 ustawy o ochronie danych osobowych wskazuje informacje, które musi zawierać zgłoszenie administratora bezpieczeństwa informacji do rejestracji. Zgodnie z art. 46f tej ustawy minister właściwy do spraw administracji publicznej określił, w drodze rozporządzenia, wzory zgłoszeń administratora bezpieczeństwa informacji, o których mowa w art. 46b ust. 2 i 3 powołanej ustawy, uwzględniając konieczność zapewnienia Generalnemu Inspektorowi informacji niezbędnych do prawidłowego realizowania jego zadań. Zgłoszenia

[131] Art. 42 ust. 4 ustawy.
[132] Art. 42 ust. 3 ustawy.

powołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych dokonuje się przy użyciu formularza zgłoszenia powołania administratora bezpieczeństwa informacji, który stanowi załącznik nr 1 do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. (Dz. U. z 2014 r. poz. 1934), a zgłoszenia odwołania przy użyciu formularza zgłoszenia odwołania administratora bezpieczeństwa informacji, który stanowi załącznik nr 2 do przedmiotowego rozporządzenia. Administrator danych, który zgłosi powołanie administratora bezpieczeństwa informacji do rejestracji zobowiązany jest zgłaszać Generalnemu Inspektorowi Ochrony Danych Osobowych każdą zmianę informacji objętych zgłoszeniem w terminie 14 dni od dokonania zmiany, a także jego odwołanie w terminie 30 dni od dnia odwołania.

W okresie od 1 stycznia do 31 grudnia 2015 r. do Biura GIODO wpłynęło **22 869 zgłoszeń powołania administratora bezpieczeństwa informacji (ABI)**. W I kwartale 2015 roku takich zgłoszeń było 3068, w II kwartale 9685, w III kwartale 7995, w IV kwartale 2121.

Ponadto administratorzy danych zgłosili **369 aktualizacji** zmian informacji objętych zgłoszeniem powołania administratora bezpieczeństwa informacji, **323 odwołania** administratora bezpieczeństwa informacji oraz **133 zapytania.**

W pierwszej kolejności Departament Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych dążył do jak najszybszego zarejestrowania tych wszystkich zgłoszeń, które zostały wypełnione w sposób zgodny z przepisami prawa. **W ten sposób w 2015 roku do ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych zostało wpisanych 15531 administratorów bezpieczeństwa informacji (około 2/3)** z ogólnej liczby 22869 zgłoszeń, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych oraz zarejestrowano **58 odwołań administratora bezpieczeństwa informacji.**

Niestety mimo dość prostej i jednoznacznie określonej przepisami prawa formy zgłaszania powołania administratora bezpieczeństwa informacji, 1/3 nadesłanych zgłoszeń obarczona była brakami formalnymi lub innymi błędami. Najczęściej popełniane błędy dotyczyły zgłaszania powołania administratorów bezpieczeństwa informacji nie na urzędowym formularzu. W wielu przypadkach administratorzy danych zamiast wypełnionego urzędowego formularza przesyłali innego rodzaju dokumenty takie jak, np. upoważniania do przetwarzania danych dla administratora bezpieczeństwa informacji lub jego zastępców, różnego rodzaju akty prawne dotyczące powołania administratora bezpieczeństwa

informacji (uchwały, zarządzenia). Takie dokumenty były odsyłane administratorom danych wraz z informacją o prawidłowej formie zgłaszania powołania administratora bezpieczeństwa informacji.

Ponadto wiele nadesłanych zgłoszeń powołania lub odwołania ABI nie zawierało wszystkich wymaganych przepisami informacji (np. nazwy administratora danych i adresu jego siedziby albo nazwiska, imienia i adresu miejsca zamieszkania oraz nr REGON, jeżeli został nadany, imienia i nazwiska administratora bezpieczeństwa informacji, podpisu pod wnioskiem), co skutkowało koniecznością wzywania wnioskodawców do usunięcia braków formalnych wniosku na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego[133].

W tej grupie nieprawidłowych zgłoszeń powołania ABI znalazło się wiele takich, które zawierały braki polegające na niezakreśleniu wszystkich lub niektórych pól oznaczających oświadczenie administratora danych o spełnieniu przez niego warunków określonych w ustawie. Takie zgłoszenia również wymagały wezwania do uzupełnienia braków formalnych nie tylko z ww. względów proceduralnych, ale także dlatego, że nie jest możliwe dokonanie wpisu w rejestrze w sytuacji, gdy zgłoszony administrator bezpieczeństwa informacji nie spełnia rygorów kwalifikacyjnych (art. 36a ust. 5 ustawy) lub nie zachowano podległości administratora bezpieczeństwa informacji bezpośrednio kierownikowi jednostki organizacyjnej (art. 36 a ust. 7 ustawy). Co istotne, zgodnie z art. 46d ust 2 pkt 1 ustawy, niespełnienie wymogów określonych w art. 36a ust. 5 i 7 ustawy stanowi przesłankę wykreślenia administratora bezpieczeństwa informacji z rejestru oraz - stosownie do art. 46e ust 1 pkt 2 ustawy - odmowy wpisania do rejestru ponownie zgłoszonego administratora bezpieczeństwa informacji, co następuje w drodze decyzji administracyjnej. Organ rejestrowy nie może bowiem dopuścić do wpisu w rejestrze w sytuacji wady prawnej, powodującej ustawowy obowiązek usunięcia takiego wpisu.

Wiele zgłoszeń, które wpłynęły do Generalnego Inspektora Ochrony Danych Osobowych w okresie sprawozdawczym było obarczonych błędami takimi jak: powołanie na administratora bezpieczeństwa informacji osoby będącej kierownikiem jednostki organizacyjnej (osoby zarządzającej podmiotem posiadającym status administratora danych),

[133] Zgodnie z art. 22 ustawy o ochronie danych osobowych postępowanie w sprawach uregulowanych w ustawie prowadzi się wg przepisów Kodeksu postępowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej. Zgodnie z art. 63 § 2 K.p.a. podanie powinno zawierać co najmniej wskazanie osoby, od której pochodzi, jej adres i żądanie oraz czynić zadość innym wymaganiom ustalonym w przepisach szczególnych. Stosownie do treści art. 63 § 3 K.p.a. podanie wniesione pisemnie powinno być podpisane przez wnoszącego.

zgłoszenie powołania więcej niż jednego administratora bezpieczeństwa informacji oraz zgłoszenie powołania zastępcy administratora bezpieczeństwa informacji.

Wobec tego rodzaju błędów Generalny Inspektor uznawał, że niedopuszczalne jest powołanie na administratorów bezpieczeństwa informacji osób będących kierownikami jednostki organizacyjnej (lub osób zarządzających podmiotami posiadającymi status administratora danych), takich jak np. dyrektorów szkół, wójtów, członków zarządu spółki, członków zarządu stowarzyszenia. Mając na uwadze podstawowe założenia znowelizowanych przepisów dotyczących administratorów bezpieczeństwa informacji Generalny Inspektor uznał, że istotną sprawą jest wymóg zapewnienia niezależnego wykonywania zadań przez ABI w celu uniknięcia sytuacji, w których administrator bezpieczeństwa informacji nadzoruje i kontroluje samego siebie. Zapewnienie niezależności osobie sprawującej wewnętrzną kontrolę przestrzegania przepisów o ochronie danych osobowych wyklucza w praktyce sprawowanie funkcji administratora bezpieczeństwa informacji przez osoby kierujące podmiotem będącym administratorem danych. Przyjęcie powyższego stanowiska uzasadnione było ponadto kompetencjami kontrolnymi administratora bezpieczeństwa informacji przewidzianymi przez znowelizowane przepisy (sprawdzenia, w tym sprawdzenia dokonywane na wezwanie Generalnego Inspektora na podstawie art. 19b ustawy o ochronie danych osobowych). Między innymi w tym celu nowelizacja wprowadziła wzmocnienie władztwa administratora bezpieczeństwa informacji chociażby przez formalnie wysokie umiejscowienie administratora bezpieczeństwa informacji w strukturze organizacyjnej administratora danych (bezpośrednia podległość administratora danych) oraz zapewnioną organizacyjną odrębność. Administrator bezpieczeństwa informacji musi mieć zapewnioną możliwość podejmowania koniecznych działań wynikających z negatywnych wyników dokonywanych przez niego sprawdzeń zgodności przetwarzania danych osobowych z przepisami prawa. Powierzenie administratorowi bezpieczeństwa informacji przez Generalnego Inspektora wykonywania czynności polegających na sprawdzeniu zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych może następować jedynie przy założeniu, że nie chodzi o sprawdzenie (kontrolowanie) samego siebie. Ponadto administrator danych, który powołał administratora bezpieczeństwa informacji, zwolniony został z obowiązków zgłaszania zbiorów danych Generalnemu Inspektorowi, na co składa się zwolnienie z obowiązków zgłoszenia nowo utworzonych zbiorów (art. 43 ust. 1a ustawy) oraz aktualizacji informacji dotyczących dotychczas zgłoszonych zbiorów (ze względu na odesłanie zawarte w art. 41 ust. 4 ustawy).

Powołany administrator bezpieczeństwa informacji ma prowadzić uproszony rejestr zbiorów danych (administratora danych) jawny dla wszystkich osób zainteresowanych.

W odniesieniu do zgłoszeń powołania na ABI przez jednego administratora danych więcej niż jednej osoby, Generalny Inspektor zwracał się do administratora danych o wskazanie, kto pełni funkcję administratora bezpieczeństwa informacji. Zgodnie bowiem z obowiązującymi przepisami może być powołany tylko jeden administrator bezpieczeństwa informacji. Przepis art. 36a ust. 1 ustawy, który stanowi, że administrator danych może powołać administratora bezpieczeństwa informacji, wyraźnie posługuje się określeniem „administratora bezpieczeństwa informacji" w liczbie pojedynczej (inaczej niż ma to miejsce w przypadku zastępców administratora bezpieczeństwa informacji)[134]. Ustawodawca przewidział zatem możliwość powołania jednego administratora bezpieczeństwa informacji oraz jednego do kilku zastępców administratora bezpieczeństwa informacji. W ocenie Generalnego Inspektora należało złożyć, że zamysłem ustawodawcy było wzmocnienie pozycji i odpowiedzialności administratora bezpieczeństwa informacji oraz umiejscowienie ośrodka koordynacji kontroli i nadzoru procesów przetwarzania danych osobowych w jednej osobie. Ponadto przyjęcie literalnej wykładni powołanych przepisów służy uniknięciu wątpliwości, kto u danego administratora danych odpowiedzialny jest za prowadzenie rejestru zbiorów danych zwolnionych z obowiązku rejestracji u Generalnego Inspektora oraz komu należy zlecać dokonywanie sprawdzeń na podstawie art. 19b ust 1 ustawy. Ponadto nawet u administratorów danych o złożonej, rozczłonkowanej strukturze zarówno dla administratora danych, jak i podmiotów danych oraz dla Generalnego Inspektora jasne będzie, kto jest osobą odpowiedzialną za realizację art. 36a ust. 2 ustawy, to jest zarówno za kompleksowe zapewnianie przestrzegania przepisów o ochronie danych osobowych, jak i wykonanie wszystkich szczegółowych zadań wymienionych w tym przepisie i służących osiągnięciu tego celu. Taka interpretacja zbieżna jest również z dążeniem Generalnego Inspektora do podniesienia jakości procesu przetwarzania i bezpieczeństwa danych oraz wzmocnienia zaufania do administratorów danych ze strony podmiotów danych.

W odniesieniu do nadsyłanych w okresie sprawozdawczym zgłoszeń powołania zastępcy administratora bezpieczeństwa informacji, Generalny Inspektor informował administratorów danych, że zgodnie z obowiązującymi przepisami zastępca administratora

[134] art. 36a ust. 6 ustawy o ochronie danych osobowych Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w art. 36a ust. 5 ustawy o ochronie danych osobowych.

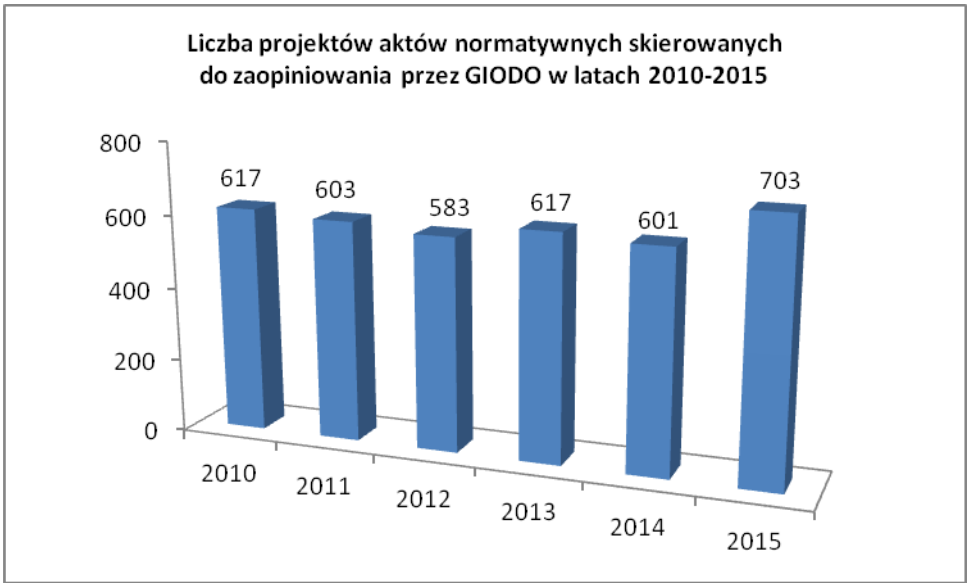
bezpieczeństwa informacji nie podlega obowiązkowi rejestracji. W ocenie Generalnego Inspektora przepis art. 46b ustawy o ochronie danych osobowych nie pozostawia wątpliwości, że zgłoszeniu do rejestracji Generalnemu Inspektorowi podlega jedynie powołanie i odwołanie administratora bezpieczeństwa informacji, nie zaś jakichkolwiek innych osób, w tym zastępców administratora bezpieczeństwa informacji.

W okresie sprawozdawczym, w przypadku nieprawidłowych zgłoszeń obarczonych brakami formalnymi lub innymi błędami, Departament Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych wysłał **pisma do administratorów danych z wezwaniem do uzupełnienia braków formalnych lub korekty innych błędów w zakresie powołania lub zgłoszenia administratora bezpieczeństwa informacji**. W odpowiedzi na tego rodzaju pisma do Biura GIODO napływają skorygowane zgłoszenia umożliwiające dokonanie rejestracji kolejnych administratorów bezpieczeństwa informacji.

8. 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.

W roku 2015 w Biurze GIODO przeanalizowano **703 projekty aktów** prawnych, czyli o 102 więcej niż w poprzednim roku sprawozdawczym. Należy zwrócić uwagę, że tylko 26 projektów było analizowanych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, gdyż nie zostały przekazane przez projektodawcę do uzgodnienia bądź konsultacji. W porównaniu do 2014 r. oznacza to pięciokrotny spadek liczby projektów opiniowanych z urzędu.



Wykres 33: ***Liczbowe zestawienie projektów aktów normatywnych skierowanych do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2010-2015.***

W 2015 roku Generalny Inspektor Ochrony Danych Osobowych brał udział w opiniowaniu **projektu ustawy o nieodpłatnej pomocy prawnej i informacji prawnej**[135]. Organ zwrócił uwagę, iż przy realizacji zadań określonych w projekcie ustawy dochodzić będzie do przetwarzania niekiedy bardzo szczegółowych informacji związanych ze sprawami, w których udzielana jest pomoc lub informacja prawna, a zatem również do przetwarzania danych osobowych. Generalny Inspektor odniósł się do projektowanego katalogu danych osobowych udostępnianych w oświadczeniach składanych przez osoby uprawnione do uzyskania nieodpłatnej pomocy prawnej (tj. imię i nazwisko, adres zamieszkania oraz PESEL), wskazując – z powołaniem się na zasadę adekwatności (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych - iż należy rozważyć, czy podawanie w tych oświadczeniach numeru PESEL jest rzeczywiście niezbędne i należycie uzasadnione.

Organ zauważył ponadto, iż doprecyzowania wymaga kto będzie gromadził dane osobowe osób korzystających z nieodpłatnej pomocy prawnej. Art. 3 ust. 9 projektu wskazywał wprawdzie, iż oświadczenia, o których mowa w ust. 4 i 5, przechowuje się w warunkach uniemożliwiających dostęp do nich osób trzecich, jednak nie wyjaśniał kto uzyskuje status administratora zebranych w ten sposób danych osobowych. Ponadto biorąc pod uwagę treść art. 26 ust. 2 pkt 4 ustawy o ochronie danych osobowych - zgodnie z którym dane powinny być przechowywane w postaci umożliwiającej identyfikację osób, których

[135] DOLiS-033-483/14

dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania - należało również określić okres przechowywania wyżej wymienionych oświadczeń.

Zgodnie z art. 17 ust. 1 pkt 4 projektu, treść rozmów prowadzonych z użyciem infolinii, za pośrednictwem której udziela się informacji prawnej, miała być utrwalana. Wyjaśnienia wymagało przede wszystkim, czy warunkiem udzielenia takiej informacji było podanie przez osobę fizyczną określonych danych osobowych. Niezależnie jednak od istnienia takiego wymogu, biorąc pod uwagę, że utrwalanie treści rozmowy każdorazowo może się wiązać z przetwarzaniem danych osobowych, w tym również tzw. danych szczególnie chronionych, Generalny Inspektor zauważył, iż wskazane byłoby szczegółowe określenie warunków ich przetwarzania w przepisach ustawy. Zgodnie bowiem z art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych wrażliwych powinno mieć podstawę w przepisach rangi ustawowej, które stwarzają pełną gwarancję ich ochrony.

Projekt ustawy przewidywał określenie w drodze rozporządzeń wymogów odnoszących się do dokumentowania udzielenia pomocy prawnej w zakresie danych dotyczących czasu trwania, przedmiotu i formy pomocy prawnej, w tym wzór karty pomocy prawnej oraz wymogów odnoszących się do dokumentowania udzielenia informacji prawnej dotyczące przedmiotu udzielonej informacji, w tym wzór karty informacji prawnej. Wyjaśnienia wymagało czy dokumentacja udzielenia pomocy prawnej i informacji będzie się wiązała z przetwarzaniem danych osobowych, w szczególności jakie ewentualnie dane miałyby się znajdować na kartach pomocy prawnej i informacji prawnej. Z uwagi na fakt, iż w związku ze sporządzaniem takiej dokumentacji może dochodzić do przetwarzania danych szczególnie chronionych, odpowiednie regulacje w tym zakresie powinny być zawarte w przepisach rangi ustawowej. Zastrzeżenia Generalnego Inspektora Ochrony Danych Osobowych budził również fakt, iż dokumentacja udzielenia pomocy prawnej (w tym również oświadczenia składane przez osoby uprawnione) oraz informacji prawnej przekazywana była odpowiednio staroście lub wojewodzie. O ile zrozumiałe było przekazywanie danych statystycznych czy też zanonimizowanych informacji dotyczących konkretnych przypadków udzielanej pomocy lub informacji prawnej (a zatem takich informacji, które nie będą stanowić danych osobowych w rozumieniu art. 6 ustawy o ochronie danych osobowych), o tyle nie znajduje uzasadnienia przekazywanie wyżej wymienionym organom również danych osobowych. W projekcie ustawy brak było przepisów, które regulowałyby cele, dla których dane zindywidualizowane miałyby być przetwarzane przez starostę lub wojewodę.

Generalny Inspektor zasugerował ponadto poddanie projektowanych przepisów analizie pod względem zgodności z regulacjami zawartymi w ustawie z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2014 r. poz. 635 z późn. zm.) oraz w ustawie z dnia 6 lipca 1982 r. o radcach prawnych (Dz. U. 2014 r. poz. 637 z późn. zm.). Art. 6 ust. 1 ustawy Prawo o adwokaturze stanowi, iż adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Zgodnie zaś z art. 3 ust. 3 ustawy o radcach prawnych, radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej. A zatem udzielenie takiej pomocy prawnej związane jest z koniecznością zachowania w tajemnicy także danych osobowych, które powinny być rozumiane nie tylko jako dane identyfikujące osobę, ale jako wszelkie informacje dotyczące określonego stanu objętego pomocą prawną. Sytuacja, w której dostęp do informacji pozyskanej przed adwokata lub radcę prawnego uzyskałyby inne podmioty, byłaby niezgodna z obecnym stanem prawnym i obowiązkiem zachowania tajemnicy zawodowej.

Uwagi organu do spraw ochrony danych osobowych zostały w większości uwzględnione. Ustawa została podpisana przez Prezydenta RP dnia 25 sierpnia 2015 r. (jako ustawa o nieodpłatnej pomocy prawnej oraz edukacji prawnej) i weszła w życie z dniem 1 stycznia 2016 r.

Jednym z ważniejszych opiniowanych przez GIODO projektów legislacyjnych był **projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw**[136]. Nowelizacja miała na celu wykonanie wyroku Trybunału Konstytucyjnego (TK) z dnia 30 lipca 2014 r. (sygn. akt K 23/11), w którym za niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji uznane zostały niektóre przepisy ustaw: o Policji, o Straży Granicznej, o kontroli skarbowej, o Żandarmerii Wojskowej i wojskowych organach porządkowych, o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, o Centralnym Biurze Antykorupcyjnym oraz o Służbie Celnej, w zakresie, w jakim nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy Prawo telekomunikacyjne.

W opiniowanym projekcie ustawy zaproponowano, aby podmiotami wyznaczonymi do kontroli nad uzyskiwaniem danych telekomunikacyjnych zostały sądy okręgowe oraz

[136] DOLiS-033-284/15

wojskowe sądy okręgowe. Generalnego Inspektor uznał, iż zaproponowana forma kontroli jest niewystarczająca – Policja i służby nie otrzymały innych nowych obowiązków poza przekazywaniem sądom raz na 6 miesięcy sprawozdań obejmujących liczbę i rodzaj pozyskanych danych telekomunikacyjnych lub pocztowych, podstawę prawną ich pozyskania i rodzaje przestępstw, w związku z którymi wystąpiono o dane. Sądy jedynie fakultatywnie zapoznawałyby się z materiałami uzasadniającymi udostępnianie danych, a uprzednia kontrola miałaby mieć miejsce wyłącznie wtedy, gdy z materiałów sprawy wynikałoby, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 §2 Kodeksu postępowania karnego. Co do zasady, proponowany w projekcie model w rzeczywistości przewidywał jedynie fakultatywną kontrolę następczą, co nie mogło zostać uznane za należyte wykonanie wyroku Trybunału Konstytucyjnego. Generalny Inspektor Ochrony Danych Osobowych postulował wprowadzenie jako zasady każdorazowej, obowiązkowej oceny adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych, wskazując przy tym, iż kontrola następcza powinna być traktowana jako wyjątek i stosowana jedynie w sprawach niecierpiących zwłoki.

Za niedostateczną realizację wyroku Trybunału Konstytucyjnego GIODO uznał przepisy ograniczające czas przeprowadzania kontroli operacyjnej przez Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Zgodnie ze stanowiskiem Trybunału, „ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. (…). W demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw – prowadzenie czynności operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów”. Tymczasem, w przypadku wyżej wymienionych służb, dopuszczalne byłoby wydawanie kolejnych postanowień o przedłużeniu kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy (bez ograniczenia, że może być to tylko jedno postanowienie). W praktyce proponowane rozwiązanie stwarzało zatem możliwość bezterminowego prowadzenia czynności operacyjno-rozpoznawczych, co stoi w sprzeczności ze standardami konstytucyjnymi i intencją Trybunału.

W uzasadnieniu do wyroku Trybunał Konstytucyjny podkreślił również, że niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania

daleko idących gwarancji proceduralnych – przede wszystkim powinien istnieć obowiązek późniejszego poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat. Na konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r. sygn. S 2/06). Z uwagi na powyższe, Generalny Inspektor wskazał na potrzebę uzupełnienia projektu o obowiązek informacyjny wobec osób, których dane zostały pozyskane przez Policję i służby.

GIODO przypomniał jednocześnie, iż kwestia sięgania przez Policję i służby po dane telekomunikacyjne nie może zostać uregulowana w sposób prawidłowy bez odniesienia się do wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 8 kwietnia 2014 r., stwierdzającego nieważność dyrektywy 2006/24 w sprawie zatrzymywania danych w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland. TSUE uznał nieważność dyrektywy ze względu na naruszenie art. 7 (poszanowanie życia prywatnego i rodzinnego) i 8 (ochrona danych osobowych) w zw. z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej. Jako przyczynę nieważności dyrektywy Trybunał wskazał brak proporcjonalności zawartych w niej rozwiązań, które, mimo iż adekwatne do celu, który ma zostać za ich pomocą osiągnięty, ingerują zbyt głęboko w prawa podstawowe. TSUE uznał, że ten sam cel (zwalczanie poważnej przestępczości oraz zapewnienie bezpieczeństwa publicznego) można było osiągnąć środkami, które w mniejszym stopniu ingerują w prawa obywateli. Mimo iż wyrok w sprawie Digital Rights Ireland nie powoduje automatycznie nieważności aktów prawa krajowego implementujących dyrektywę 2006/24, to konieczne było uwzględnienie go w pracach legislacyjnych nad projektem ustawy, który dotyczył tej samej materii. Tymczasem, zaproponowanych w senackim projekcie rozwiązań nie można było uznać za zgodne z wytycznymi Trybunału Sprawiedliwości Unii Europejskiej.

Ostatecznie projekt z lipca 2015 r. nie został przyjęty. W grudniu 2015 r. do Sejmu wpłynął **poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw**[137], który w większości powielał zaproponowane w senackim projekcie rozwiązania, wobec czego Generalny Inspektor podtrzymywał zgłaszane wcześniej zastrzeżenia. Jako najważniejsze różnice miedzy projektami, do których GIODO zgłosił dodatkowe zastrzeżenia można wskazać:

[137] DOLiS-033-640/15

- szerszy zakres sytuacji, w których można sięgać po dane (brak ograniczenia do pozyskiwania danych w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów **poważnych** przestępstw);
- przepisy nowego projektu przewidywały również, obok możliwości pozyskiwania danych telekomunikacyjnych i pocztowych, możliwość sięgania po dane internetowe (czyli dane określone w art. 18 ust. 1-5 ustawy o świadczeniu usług drogą elektroniczną);
- brak jakiejkolwiek kontroli uprzedniej sięgania po dane – wg projektu senackiego uprzednia kontrola miała mieć miejsce wtedy, gdy z materiałów sprawy wynikałoby, że konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych dotyczących bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 §2 Kodeksu postępowania karnego;
- w ramach kontroli następczej projekt senacki przewidywał, że w przypadku stwierdzenia przez sąd braku podstaw do pozyskania danych, podlegają one niezwłocznie zniszczeniu. Projekt poselski nie wspominał o weryfikacji zasadności pozyskania danych ani o sposobie postępowania z danymi pozyskanymi niezgodnie z prawem. Przewidziano jedynie, że sąd może zapoznać się z materiałami uzasadniającymi udostępnienie danych danemu podmiotowi i informuje następnie ten podmiot o wynikach kontroli.

Ustawa o zmianie ustawy o Policji oraz niektórych innych ustaw została podpisana przez Prezydenta RP dnia 3 lutego 2016 r. Zgłaszane przez Generalnego Inspektora uwagi nie zostały uwzględnione.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zgłosił szereg uwag do **projektu ustawy o pomocy państwa w wychowywaniu dzieci**[138]. Organ skrytykował m.in. zbyt ogólnie sformułowany i niejasny art. 8 projektu, który stanowił, iż w przypadku, gdy organ właściwy powziął informację, że osoba uprawniona do świadczenia wychowawczego lub jej przedstawiciel marnotrawią wypłacane jej świadczenie lub wydatkują je niezgodnie z przeznaczeniem, organ właściwy przekazuje należne osobie świadczenie w całości lub w części w formie rzeczowej. O ile zrozumiałe jest, iż świadczenie dotyczy konkretnego celu, jakim jest wychowanie dzieci i zgodnie z tym celem powinno być wydatkowane, o tyle rozważenia wymaga sposób sprawowania ewentualnej kontroli w tym

[138] DOLiS-033-616/15

zakresie, tak, by nie godził on w podstawowe prawa jednostek. Przede wszystkim, nie było jasne skąd organ właściwy miałby pozyskiwać informację o marnotrawieniu lub wydatkowaniu niezgodnie z przeznaczeniem świadczenia wychowawczego oraz jak miałoby być rozumiane pojęcie „marnotrawienie".

Zgodnie z art. 10 ust. 2 projektu, organ właściwy mógł upoważnić swojego zastępcę, pracownika urzędu albo kierownika ośrodka pomocy społecznej lub innej jednostki organizacyjnej gminy, a także inną osobę na wniosek kierownika ośrodka pomocy społecznej lub innej jednostki organizacyjnej gminy, do prowadzenia postępowania w sprawach świadczenia wychowawczego, a także do wydawania w tych sprawach decyzji. W opinii organu przepis ten nie był wystarczająco precyzyjny. Przykładowo, określenie „inna jednostka organizacyjna gminy" jest zbyt ogólne, obejmuje bowiem również takie podmioty jak np. szkoły czy instytucje kultury, a ze względu na specyfikę regulowanego obszaru uzasadnione wydaje się stwierdzenie, że tylko niektóre jednostki organizacyjne mogą zostać upoważnione do prowadzenia postępowania w sprawach świadczenia wychowawczego oraz do wydawania w tych sprawach decyzji. Powołany przepis powinien wprost wskazywać takie jednostki.

Generalny Inspektor odniósł się również do przepisów dotyczących wniosku o ustalenie prawa do świadczenia wychowawczego – wskazując, iż należy zadbać o to, by zakres danych, jakie muszą się znaleźć w tym wniosku, był w przepisach ustawy określony w sposób jednoznaczny. Jest to szczególnie istotne w sytuacji, gdy wniosek miałby również zawierać informacje na temat niepełnosprawności dziecka, a zatem dane szczególnie chronione (wrażliwe). Należało ponadto doprecyzować, czy we wniosku miałyby się znajdować również dane osoby sprawującej opiekę nad dzieckiem wspólnie z osobą składającą wniosek.

Art. 14 ust. 2 projektu przewidywał utworzenie przez ministra właściwego do spraw rodziny rejestru centralnego obejmującego m.in. dane dotyczące osób pobierających świadczenie wychowawcze, osób ubiegających się o świadczenie wychowawcze oraz członków ich rodzin. Niepokojący z punktu widzenia ochrony danych osobowych był fakt, iż w uzasadnieniu do projektu w żaden sposób nie odniesiono się do tej kwestii – nie wykazano celowości i niezbędności planowanego rozwiązania. W tym kontekście GIODO podkreślił, iż każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania (*privacy by design*). Ponadto, jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający

przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych (*privacy impact assessment*). W ramach takiej oceny należy między innymi rozważyć, czy za pośrednictwem rejestru nie będzie dochodziło do profilowania osób czy też pewnych zjawisk lub zachowań.

Organ wskazał zatem, iż *„niezbędna jest analiza zasadności gromadzenia danych osobowych na poziomie centralnym – biorąc pod uwagę okoliczność, iż ustalanie prawa do świadczenia wychowawczego odbywać się będzie na poziomie gminy (...) Art. 51 ust. 2 Konstytucji RP stanowi, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Stąd regulacje prawne muszą precyzyjnie określać zakres danych osobowych oraz cele, dla których będą one przetwarzane. Niewątpliwie cel i zakres pozyskiwanych danych powinien być podporządkowany zadaniom nałożonym na podmioty publiczne realizujące zadania w omawianym obszarze. Tylko wtedy bowiem zakres zbieranych danych nie będzie przekraczać kryterium niezbędności w demokratycznym państwie prawnym”*.

Ponadto w opinii Generalnego Inspektora rozważenia wymagało, na ile niezbędna jest konstrukcja zezwalająca na udostępnianie innym podmiotom zgromadzonych w rejestrze centralnym informacji, zaproponowana w art. 14 ust. 4 projektu. Jako cel projektowanej ustawy wskazana została pomoc finansowa kierowana do rodzin wychowujących dzieci, tymczasem obok regulacji uzasadnionych realizacją powyższego celu, projektodawca zawarł rozwiązania pozwalające na udostępnianie różnym podmiotom, w zakresie niezbędnym do realizacji ich zadań ustawowych, informacji zawartych w rejestrze centralnym. Organ podkreślił, iż przyznawanie świadczeń o charakterze socjalnym nie powinno wiązać się ze zwiększeniem uprawnień nadzorczych wobec osób, które uzyskały do tych świadczeń prawo i odbywać się kosztem ich prawa do prywatności.

Również okresy retencji danych (art. 14 ust. 5 i 6 projektu ustawy) nie zostały w żaden sposób uzasadnione. Generalny Inspektor poddał w wątpliwość konieczność przechowywania takich informacji przez okres 10 lat od dnia zaprzestania udzielania świadczenia wychowawczego oraz 1 roku w przypadku, gdy świadczenie nie zostało przyznane oraz 10 lat od momentu ich udostępnienia z rejestru centralnego. W ocenie organu do spraw ochrony danych osobowych było to sprzeczne z podstawową zasadą ograniczenia czasowego przetwarzania danych, wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych.

Art. 35 pkt 8 przewidywał zmianę w ustawie o świadczeniach rodzinnych, polegającą na uchyleniu art. 23 ust. 4a, a tym samym likwidacji tzw. krótkiego wywiadu

środowiskowego, który, w razie zaistnienia wątpliwości, mógł być stosowany do weryfikacji faktu samotnego wychowywania dziecka przez osobę ubiegającą się o świadczenie rodzinne (zgodnie z art. 20t ust. 8 ustawy o systemie oświaty ten rodzaj wywiadu mógł być również przeprowadzany w związku z rekrutacją do przedszkoli, szkół i innych placówek). Jak wynikało z uzasadnienia do projektu ustawy, do weryfikacji tej okoliczności miałby być stosowany wyłącznie rodzinny wywiad środowiskowy, o którym mowa w przepisach o pomocy społecznej. Zdaniem Generalnego Inspektora, weryfikacja faktu samotnego wychowywania dziecka w formie pełnego wywiadu środowiskowego stanowić mogłaby nadmierną, nieproporcjonalną ingerencję w prywatność jednostek. Zakres danych gromadzonych podczas przeprowadzania rodzinnego wywiadu środowiskowego jest znacznie szerszy niż zakres informacji wynikających z kwestionariusza wywiadu przeprowadzanego na podstawie art. 23 ust. 4a ustawy o świadczeniach rodzinnych – obejmuje m.in. stan zdrowia, niepełnosprawność, karalność, wysokość dochodu, itp. Zachodzi wątpliwość, czy tak szeroki katalog danych jest rzeczywiście niezbędny z punktu widzenia celu, jakim jest ustalenie, czy osoba ubiegająca się o świadczenie rodzinne rzeczywiście samotnie wychowuje dziecko. Powstało również pytanie, jak miałaby przebiegać weryfikacja tej okoliczności w związku z rekrutacją do przedszkoli, szkół i innych placówek, bowiem projekt ustawy nie przewidywał zmian w obowiązującym art. 20t ust. 8 ustawy o systemie oświaty.

Generalny Inspektor zgłaszał również uwagi do kolejnych wersji projektu, co miało miejsce w kolejnym okresie sprawozdawczym. Ze stanowczym sprzeciwem organu spotkało się zwłaszcza wprowadzenie zmian do przepisów ustawy o ochronie danych osobowych. Niestety, uwagi te nie zostały uwzględnione. Ustawa została podpisana przez Prezydenta RP w dniu 17 lutego 2016 r.

Generalny Inspektor Ochrony Danych Osobowych otrzymał w okresie sprwazdawczym do zaopiniowania **projekt ustawy o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw**[139]. Kwestie regulowane przez projekt w pewnym zakresie były już opiniowane przez Generalnego Inspektora w ramach uzgodnień projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia (sygnatura DOLiS-033-340/14). Przyjmując z zadowoleniem uwzględnienie przez projektodawcę części ze zgłaszanych wówczas uwag, organ do spraw ochrony danych osobowych wskazał, iż w projektowanym art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta winny zostać

[139] DOLiS-033-318/15

określone kategorie osób niewykonujących zawodów medycznych, które mogą zostać upoważnione przez administratorów danych do przetwarzania danych zawartych w dokumentacji medycznej oraz cele dla realizacji których takie upoważnienie do przetwarzania danych może być nadane.

W projektowanych przepisach w dalszym ciągu nie została wystarczająco doprecyzowana kwestia sposobu postępowania z dokumentacją medyczną po likwidacji podmiotu leczniczego albo zakończeniu działalności leczniczej przez lekarza lub pielęgniarkę, którzy wykonywali zawód w ramach praktyki zawodowej. Według projektowanego art. 30a ust. 2 pkt 2, w przypadku podmiotu leczniczego innego niż określony w pkt 1 oraz praktyki zawodowej (i przy jednoczesnym braku podmiotu przejmującego zadania po podmiocie, który zaprzestał udzielania świadczeń zdrowotnych) za przechowywanie i udostępnianie dokumentacji medycznej miał odpowiadać podmiot udzielający świadczeń zdrowotnych, z którym podmiot zaprzestający udzielania świadczeń zawarł umowę o przechowywanie dokumentacji medycznej. Tymczasem, dotyczące tej kwestii odpowiednio art. 106 ust. 3 pkt 10 a ustawy z dnia 15 kwietnia 2011 roku o działalności leczniczej (Dz. U. z 2013 r. poz. 217, z późn. zm.) i art. 106 ust. 4 pkt 8 a ustawy o działalności leczniczej ograniczają się jedynie do nałożenia obowiązku wskazania we wniosku rejestracyjnym miejsca przechowywania dokumentacji medycznej w wyżej wskazanych przypadkach, nie określają jednak, czy konieczne jest zawarcie w tym zakresie stosownej umowy oraz pozostawiają pełną dowolność przy wyborze tego miejsca i nie nadają organowi rejestrującemu kompetencji do weryfikowania prawidłowości wskazanego miejsca. Nie jest zatem jasny sposób postępowania z dokumentacją w przypadku podmiotów, których dotyczy projektowany art. 30a ust. 2 pkt 2, a które nie zawarły umowy o przechowywanie dokumentacji medycznej (skoro obowiązek jej zawarcia *de facto* nie istnieje). Na potrzebę zawężenia bądź uściślenia miejsc, w których może odbywać się przechowywanie dokumentacji medycznej po zaprzestaniu udzielania świadczeń zdrowotnych przez podmiot, Generalny Inspektor wskazywał również w uwagach do projektu założeń do projektu ustawy o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw (pismo z dnia 7 grudnia 2013 r. sygn. DOLiS-033-496/13/AFS/82310). Zgodnie z odpowiedzią Ministerstwa Zdrowia z dnia 24 lutego 2014 r. (MZ-OZZ-077-29555-40/AWI/14), w przypadku zakończenia działalności przez podmioty lecznicze inne niż podmioty niebędące przedsiębiorcami, funkcję „przechowawcy" miały sprawować podmioty lecznicze, których statuty przewidują wykonywanie tego rodzaju działalności. Uregulowanie

zawarte w projektowanym art. 30a ust. 2 pkt 2 i brak stosownych ograniczeń dotyczących miejsca przechowywania dokumentacji wpisywanego do rejestru zgodnie z powołanymi wyżej art. 106 ust. 3 pkt 10 a oraz art. 106 ust. 4 pkt 8 a ustawy o działalności leczniczej, daje w praktyce możliwość pełnej dowolności w wyborze takiego miejsca – co biorąc pod uwagę specyfikę danych zawartych w dokumentacji medycznej, nie może zyskać akceptacji Generalnego Inspektora.

Doprecyzowania wymaga również sposób postępowania z dokumentacją w przypadku opisanym w projektowanym art. 30a ust. 5, a mianowicie jakie działania w tym zakresie podejmuje po uzyskaniu stosownej informacji właściwy oddział wojewódzki Narodowego Funduszu Zdrowia.

Przyjmując z zadowoleniem fakt zainicjowania przez projektodawcę działań legislacyjnych zmierzających do ustalenia zasad dopuszczalności outsourcingu przechowywania dokumentacji medycznej, Generalny Inspektor Ochrony Danych Osobowych stwierdził, iż ocena zaproponowanych rozwiązań wypada – zasadniczo – pozytywnie. W opinii Generalnego Inspektora poprawienia wymagał jednak art. 30a ust. 9, gdyż obowiązek zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją umowy powierzenia przetwarzania danych, winien dotyczyć osób, które uzyskają u zleceniobiorcy faktyczny dostęp do danych w następstwie zawarcia tej umowy, nie zaś samego podmiotu, któremu przetwarzanie danych zostało powierzone. Nadal pozostaje jednak nieuregulowana kwestia outsourcingu przechowywania dokumentacji medycznej w przypadkach innych niż te, o których mowa w projektowanym art. 30a, mimo iż takie rozwiązania, zakładające stosowne zmiany w art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, znajdowały się w projekcie ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia.

Prace nad projektem zakończyły się na etapie uzgodnień międzyresortowych i konsultacji publicznych.

Generalny Inspektor Ochrony Danych Osobowych otrzymał do zaopiniowania **Kierunkowe założenia nowej ordynacji podatkowej**[140]. Organ zaprezentował szereg uwag do tego dokumentu, odnoszących się w szczególności do systemu biometrii głosowej, jaki ma być wykorzystywany w ramach nowego Systemu Informacji Telefonicznej w biurach Krajowej Informacji Podatkowej. Informacje o planach wdrożenia takiego mechanizmu nie

[140] DOLiS-033-230/15

wynikały w sposób jednoznaczny z przesłanego GIODO dokumentu (wskazano w nim jednak w sposób ogólny, iż „stworzyć należy system identyfikacji rozmówcy" oraz przewidziano rejestrowanie rozmów telefonicznych), znajdowały się natomiast w dokumentacji przetargowej dostępnej na stronie internetowej Ministerstwa Finansów. Rozwiązanie to wzbudziło szczególne zaniepokojenie Generalnego Inspektora Ochrony Danych Osobowych nie tylko ze względu na wątpliwości dotyczące jego zgodności z przepisami Konstytucji i ustawy o ochronie danych osobowych, ale również z uwagi na fakt, iż przetarg na zaprojektowanie, dostawę oraz wdrożenie systemu został rozpisany na rok przed zaprezentowaniem założeń nowej ordynacji podatkowej (która reguluje kwestie związane z funkcjonowaniem Krajowej Informacji Podatkowej), co jest sprzeczne ze ideą *privacy by design.* Wprowadzenie – bez jakiejkolwiek podstawy prawnej – systemu, którego funkcjonowanie prowadziłoby do ograniczenia konstytucyjnych wolności i praw jest ponadto niedopuszczalne z uwagi na treść art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Planowane rozwiązania polegające na nagrywaniu rozmów telefonicznych i analizie biometrycznej głosu, oprócz braku odpowiedniej podstawy prawnej, nie spełniały w opinii Generalnego Inspektora kryterium niezbędności. Zaprezentowane założenia jedynie ogólnikowo odnosiły się do kwestii stworzenia „systemu identyfikacji rozmówcy" i rejestrowania prowadzonych rozmów, nie precyzując na czym dokładnie te rozwiązania miałyby polegać i nie wykazując niezbędności ich wprowadzenia, a co za tym idzie – konieczności ograniczenia konstytucyjnych wolności i praw. Przez projektodawcę nie został wskazany cel, jakiemu miałoby służyć takie ograniczenie prawa do prywatności, a co za tym idzie – nie było jasne czy w ogóle jest ono uzasadnione. Generalny Inspektor zauważył, iż: „Projektodawca w pierwszej kolejności powinien wykazać niezbędność wprowadzenia danego rozwiązania, innymi słowy, że nie istnieje inny, mniej ingerujący w prywatność sposób realizacji danego celu. Należy zatem udowodnić, iż z uwagi na ten cel, system oparty na biometrii głosowej jest jedynym możliwym rozwiązaniem".

Rozważenia wymagało również, czy proponowany system gwarantuje równe prawa i dostęp do informacji podatkowej dla osób, które z uwagi na ochronę prywatności zdecydują

się na inną, niż telefoniczna, formę kontaktu. Nie można bowiem dopuścić do sytuacji, w której osoby decydujące się na udostępnienie swoich danych biometrycznych byłyby w praktyce traktowane w sposób bardziej uprzywilejowany od osób korzystających z innej formy kontaktu, tym bardziej jeśli chodzi o usługę, która powinna być dostępna na równych zasadach dla wszystkich podatników.

GIODO zwrócił ponadto uwagę na potencjalne zagrożenia związane ze stosowaniem biometrii głosowej – przede wszystkim z punktu widzenia bezpieczeństwa tego rodzaju identyfikacji i ryzyka związanego z możliwością przechwycenia próbki głosu. Bez odpowiednich zabezpieczeń i funkcji pozwalających na identyfikowanie oszustw, rozwiązanie zaprojektowane jako ułatwiające kontakt podatnika z administracją, w praktyce wiązałoby się z licznymi zagrożeniami.

Dopiero po określeniu celu i wykazaniu niezbędności ingerencji w prywatność, możliwe będzie dokonanie analizy proponowanych rozwiązań z zasadami ochrony danych osobowych. Jak wskazano powyżej, dane biometryczne stanowią dane osobowe, w związku z czym ich przetwarzanie musi mieć miejsce w zgodzie z obowiązującymi przepisami ustawy o ochronie danych osobowych i aktów wykonawczych.

Generalny Inspektor przypomniał jednocześnie, iż przepisy ustawy Prawo telekomunikacyjne przewidują ochronę tajemnicy telekomunikacyjnej, a w szczególności wprowadzają zasadę, zgodnie z którą zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu (art. 159 ust. 2), chyba że m.in. będzie to konieczne z powodów przewidzianych ustawą lub przepisami odrębnymi (pkt 4). Jak stanowi art. 159 ust. 3, z wyjątkiem przypadków określonych ustawą, ujawnianie lub przetwarzanie treści albo danych objętych tajemnicą telekomunikacyjną narusza obowiązek zachowania tajemnicy telekomunikacyjnej.

Kierunkowe założenia ostatecznie nie przybrały formy projektu ustawy.

Odnosząc się do przedstawionego mu do zaopiniowania **projektu ustawy o rewitalizacji**[141] Generalny Inspektor Ochrony Danych Osobowych zauważył, iż nie jest jasne, czy do opracowania analiz będących podstawą sporządzenia i realizacji gminnego programu rewitalizacji będą wykorzystywane informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy o ochronie danych osobowych. Zasugerował zatem wyraźne

[141] DOLiS-033-169/15

wskazanie w przepisach projektowanej ustawy, czy informacje pozyskiwane przez wójta, burmistrza lub prezydenta miasta stanowić będą dane osobowe. Generalny Inspektor przyjął jednocześnie, że informacje, o których mowa w art. 13 ust. 1 projektu nie będą miały takiego charakteru, w związku z ograniczeniem wynikającym z art. 5 ust. 2 ustawy o dostępie do informacji publicznej, zgodnie z którym prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę 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.

Odnosząc się zaś do art. 13 ust. 2 projektu (i zmian przepisów innych ustaw proponowanych w art. 41, 49 i 50 projektu), organ wskazał, iż niezbędne jest doprecyzowanie, czy pozyskiwane na tej podstawie dane miałyby być danymi osobowymi. Wyjaśnienia wymagało przy tym, co obejmują dane dotyczące miejsca zamieszkania osoby pozyskiwane na podstawie art. 13 ust. 2 projektu oraz projektowanych zmian w przepisach ustawy o Krajowym Rejestrze Karnym, ustawy o pomocy społecznej oraz ustawy o promocji zatrudnienia i instytucjach rynku pracy. Zgodnie z art. 25 Kodeksu cywilnego miejscem zamieszkania osoby fizycznej jest miejscowość, w której osoba ta przebywa z zamiarem stałego pobytu. Generalny Inspektor wskazał, iż *„jeśli projektowane przepisy posługują się sformułowaniem „miejsce zamieszkania" w powyższym znaczeniu, zakres pozyskiwanych informacji nie wzbudza zastrzeżeń Generalnego Inspektora Ochrony Danych Osobowych, gdyż nie pozwala on na identyfikację osoby, której dane dotyczą. Jeśli zaś informacje te miałyby również obejmować ulicę, numer domu czy numer mieszkania, wówczas mogłoby dochodzić do bezpośredniej lub pośredniej identyfikacji konkretnej osoby, a co za tym idzie – do przetwarzania jej danych osobowych. Należy zatem rozważyć, czy do opracowania analiz będących podstawą sporządzenia i realizacji gminnego programu rewitalizacji rzeczywiście niezbędne jest przetwarzanie informacji stanowiących dane osobowe"*. Doprecyzowania wymagało ponadto, jakie „informacje o osobach będących na utrzymaniu osoby bezrobotnej" miałyby być pozyskiwane przez wójta, burmistrza lub prezydenta miasta zgodnie z art. 13 ust. 2 pkt 2 projektu ustawy.

Generalny Inspektor podkreślił, że w razie uznania przez projektodawcę, że przetwarzanie zindywidualizowanych danych rzeczywiście jest niezbędne, istnieje konieczność określenia w przepisach prawa przypadków, w jakich to następuje oraz określenia w nich, w jaki sposób wykazywana będzie niezbędność uzyskania tego rodzaju

informacji. Z przepisów powinien bowiem jednoznacznie wynikać cel przetwarzania danych osobowych, a przetwarzanie może dotyczyć tylko takiego rodzaju danych i tylko o takiej treści, które są niezbędne ze względu na ten cel.

Wyjaśnienia wymagało również, jak będzie wyglądało dalsze ewentualne przetwarzanie danych dla potrzeby opracowania analizy – a zatem czy przewidywany jest bezpośredni kontakt z osobami, których te dane dotyczą oraz czy w treści sporządzonych analiz będą znajdowały się również informacje stanowiące dane osobowe (w tym tzw. dane wrażliwe, których przetwarzanie zgodnie z art. 27 ust. 1 jest co do zasady zabronione). Ten aspekt postępowania z informacjami, którymi mogą być także dane osobowe zupełnie nie został wyartykułowany w projekcie.

Na zakończenie Generalny Inspektor Ochrony Danych Osobowych wskazał, iż w jego opinii do realizacji zadania jakim jest opracowanie analiz będących podstawą sporządzenia i realizacji gminnego programu rewitalizacji nie jest niezbędne pozyskiwanie informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, czyli danych osobowych. Tym samym przepisy projektowanej ustawy powinny w jednoznaczny sposób wskazywać, iż analizy nie będą sporządzane w oparciu o dane zindywidualizowane.

Ostatecznie projektodawca zrezygnował z przetwarzania danych o charakterze jednostkowym. Prezydent RP podpisał ustawę dnia 27 października 2015 r.

Generalny Inspektor Ochrony Danych Osobowych otrzymał również do zaopiniowania kolejną wersję **projektu ustawy o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji**[142], do której zgłosił m.in. następujące uwagi:

1) odnosząc się do treści art. 24 ust. 5 projektu, Generalny Inspektor zauważył, iż niedopuszczalna jest tego typu ogólna regulacja zezwalająca na dostęp do danych „zawartych w zbiorach prowadzonych przez osoby trzecie": *„Jeśli w opinii projektodawcy konieczna jest weryfikacja roszczeń i dostęp do danych przez Fundusz, podkreślić należy, iż w odniesieniu do osób fizycznych przepisy powinny ograniczać zakres pozyskiwanych danych do rzeczywiście niezbędnych z punktu widzenia celu, jaki ma zostać zrealizowany mocą przepisów procedowanego projektu ustawy"*. Organ zwrócił uwagę na potrzebę wyraźnego określenia do jakich konkretnie zbiorów Fundusz miałby mieć dostęp. Podmiot występujący o udostępnienie określonych informacji powinien również móc wskazać podstawę prawną

[142] DOLiS-033-188/13

upoważniającą go do uzyskania danych, zaś administrator danych, udostępniając dane osobowe musi każdorazowo zweryfikować, czy istnieje postawa prawna do takiego udostępnienia. GIODO podkreślił również, iż przepisy powinny wprost określać cel, zakres i zasady takiego udostępniania danych. Wszystkie cele przetwarzania danych osobowych muszą znaleźć się w przepisach ustawy, a w przypadku tzw. danych wrażliwych (o których mowa w art. 27 ustawy o ochronie danych osobowych), szczególnie istotne jest również precyzyjne określenie zamkniętego katalogu danych osobowych, które będą dla realizacji tych celów przetwarzane. Ponadto ustawa o ochronie danych osobowych wymaga, aby dane osobowe były adekwatne w stosunku do celów, dla jakich są przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych), a zatem, aby swym rodzajem i swą treścią dane osobowe nie wykraczały poza potrzeby wynikające z celu zbierania;

2) w odniesieniu do art. 32 ust. 3, GIODO wskazał, iż przewidziana w nim weryfikacja danych w rejestrze PESEL musi mieć również odzwierciedlenie w przepisach wiążących ministra właściwego do spraw wewnętrznych i regulujących funkcjonowanie rejestru PESEL. Zatem, aby dla realizacji celów przewidzianych w projektowanej ustawie możliwe było korzystanie z rejestru PESEL, konieczne byłoby wprowadzenie stosownych zmian w przepisach ustawy o ewidencji ludności;

3) podobne wątpliwości jak wskazane w punkcie 1, wzbudziła również propozycja przedstawiona w art. 42 ust. 3 projektu, która przewidywała udostępnianie Funduszowi danych dotyczących osób i podmiotów ujętych w systemach wyliczania zawartych w zbiorach prowadzonych przez podmioty lub osoby trzecie, w szczególności dane ze zbiorów meldunkowych, zbioru danych osobowych PESEL oraz ewidencji wydanych i unieważnionych dowodów osobistych, o których mowa w odrębnych przepisach. Nie wynikało z niej bowiem, na jakich konkretnie podmiotach/organach spoczywa obowiązek udostępnienia Funduszowi danych z prowadzonych przez nie zbiorów. W opinii Generalnego Inspektora niedopuszczalne jest przyjęcie rozwiązania, które jedynie przykładowo wymienia podmioty zobowiązane do takiego działania, pomijając inne i stwarzając jednocześnie możliwość rozszerzającej interpretacji w zakresie kręgu podmiotów zobligowanych do działania związanego z przetwarzaniem danych osobowych;

4) odnosząc się do przepisów zawartych w rozdziale „Transgraniczne wypłaty środków gwarantowanych”, organ zauważył, iż przekazywanie danych osobowych, jako forma ich przetwarzania, musi opierać się na jednej z przesłanek wymienionych w art. 23 ust. 1 pkt 1-5 ustawy o ochronie danych osobowych. Z uwagi na fakt, iż forma porozumienia nie

jest w tych przepisach wskazana jako jedna z podstaw legalizujących przetwarzanie danych osobowych, GIODO uznał, iż uzasadnione byłoby doprecyzowanie w przepisach projektowanej ustawy zakresu przekazywanych danych i na jakich zasadach się ono odbywa. Regulowanie zasad przetwarzania danych osobowych nie powinno być pozostawiane aktom pozaustawowym, w szczególności dokumentom o formie i statusie nieznanym przepisom ustawy o ochronie danych osobowych, wiąże się to bowiem z ryzykiem nadużyć i dowolności w przetwarzaniu danych osobowych;

5) w odniesieniu do art. 168 ust. 8 projektu, Generalny Inspektor zauważył, iż wyłączenie stosowania tajemnicy bankowej, zawodowej, czy też ujawnienie informacji poufnej oraz informacji objętych tajemnicą przedsiębiorstwa nie może się odbywać wyłącznie na podstawie tego przepisu: *„Konieczne jest zatem wprowadzenie stosownych zmian w przepisach ustawy Prawo bankowe, ustawy o obrocie instrumentami finansowymi oraz ustawy o zwalczaniu nieuczciwej konkurencji – regulacje te muszą precyzować cele, dla których będzie miało miejsce udostępnianie danych i które jednocześnie będą spójne z celami określonymi w projektowanej ustawie”*.

Prace nad projektem nie zostały zakończone w 2015 r. – w chwili sporządzania sprawozdania był on procedowany w Parlamencie RP i do tego etapu uwagi GIODO nie zostały uwzględnione.

Generalny Inspektor Ochrony Danych Osobowych otrzymał do zaopiniowania **projekt założeń do projektu ustawy o zawodzie psychologa i samorządzie zawodowym psychologów**[143]. Odnosząc się do przedstawionego dokumentu, organ przypomniał, że dnia 22 marca 2012 r. skierował do Ministra Pracy i Polityki Społecznej wystąpienie w sprawie podjęcia prac legislacyjnych mających na celu prawne uregulowanie zasad i sposobu prowadzenia dokumentacji przez psychologów (sygn. DOLiS-035-893/12). Problem braku szczegółowych regulacji dotyczących dokumentacji psychologicznej był niejednokrotnie sygnalizowany organowi ochrony danych osobowych w kierowanych do niego pismach.

Przedmiotem zgłaszanych wątpliwości były przede wszystkim zdarzające się w praktyce przypadki odmawiania osobom korzystającym z usług psychologa udostępniania dokumentów zawierających informacje na temat tych osób, z powoływaniem się np. na tajemnicę psychologa lub wskazywaniem, że testy psychologiczne mogą być udostępniane wyłącznie specjalistom. Organ do spraw ochrony danych osobowych podtrzymał zgłoszone

[143] DOLiS-033-424/15

wówczas zastrzeżenia i postulaty oraz podkreślił, że z uwagi na fakt, iż dokumentacja psychologiczna może zawierać informacje o charakterze danych „szczególnie chronionych" (zgodnie art. 27 ust. 1 ustawy o ochronie danych osobowych), niezbędne jest kompleksowe ujęcie kwestii związanych z jej przetwarzaniem w przepisach o randze ustawy.

Generalny Inspektor wskazał przy tym, iż najważniejsze kwestie dotyczące prowadzenia rejestrów psychologów również powinny być uregulowane w przepisach rangi ustawy. Akceptacji Generalnego Inspektora nie mogło w związku z tym zyskać rozwiązanie, zgodnie z którym zakres danych podlegających wpisowi na listę psychologów miałaby określać Krajowa Rada Psychologów (s. 24 projektu założeń). Przepisy rangi ustawowej powinny regulować zasadnicze kwestie dotyczące prowadzenia zarówno Centralnego Rejestru Psychologów, jak i regionalnych rejestrów psychologów, w szczególności zaś z przepisów tych wynikać powinny następujące kwestie: podmioty decydujące o celach i środkach przetwarzanych danych, katalog danych znajdujących się w rejestrach, okres przechowywania tych danych, zasady udostępniania informacji z rejestrów, krąg podmiotów mających dostęp do danych.

Prace nad projektem zakończyły się na etapie uzgodnień międzyresortowych i konsultacji publicznych – w oparciu o projekt założeń nie został zaprezentowany projekt ustawy.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych zgłosił także uwagi do **projektu rozporządzenia Ministra Administracji i Cyfryzacji zmieniającego rozporządzenie w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej** oraz **projektu rozporządzenia Ministra Administracji i Cyfryzacji zmieniającego rozporządzenie w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej**[144].

W odniesieniu do projektu rozporządzenia Ministra Administracji i Cyfryzacji zmieniającego rozporządzenie w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej, GIODO za nieuzasadnione uznał rozszerzenie w § 3 ust. 1 projektu zakresu danych wymaganych do założenia konta przez użytkownika o numer PESEL, numer telefonu komórkowego oraz adres miejsca zamieszkania – podczas gdy w dotychczasowym stanie prawnym do założenia konta wystarczające było podanie imienia, nazwiska, adresu poczty elektronicznej oraz identyfikatora użytkownika. W uzasadnieniu

[144] DOLiS-033-218/15

projektu wskazano, iż pozyskiwanie numeru PESEL jest związane z planami połączenia procedur zakładania konta w systemie ePUAP oraz składania wniosku o potwierdzenie profilu zaufanego ePUAP. Organ ochrony danych osobowych wielokrotnie podnosił zastrzeżenia w odniesieniu do zasad posługiwania się profilem zaufanym użytkownika na Platformie ePUAP, które wiąże się z koniecznością ujawniania numeru PESEL, gdyż może to naruszyć prywatność obywatela poprzez możliwość powiązania z innymi rejestrami oraz z uwagi na semantyczność cech tego identyfikatora (data urodzenia i płeć).

Wątpliwości Generalnego Inspektora wzbudziło ponadto obligatoryjne podawanie adresu zamieszkania w celu założenia konta. O ile umożliwienie „wspierania użytkownika w zakresie wyszukiwania przez ePUAP usług właściwych terytorialnie dla zadeklarowanego adresu" wydaje się uzasadnione, o tyle powinno być ono funkcjonalnością dostępną opcjonalnie – wyłącznie dla osób, które zgodziły się na udostępnienie swojego adresu zamieszkania.

Generalny Inspektor sprzeciwił się ponadto konieczności podawania numeru telefonu komórkowego w celu założenia konta. Nie kwestionując fakultatywności podawania tej danej przez osoby, które chcą otrzymywać informacje z systemu na numer telefonu komórkowego, organ nie wyraził aprobaty wobec jej wymuszania poprzez wprowadzenie obowiązku jej udostępnienia. Obligatoryjne podawanie numeru telefonu komórkowego spowodowałoby, iż założenie konta dla użytkownika w systemie ePUAP byłoby dostępne wyłącznie dla osób, które taki numer posiadają, a tym samym ograniczałoby dostęp obywateli do usług administracji publicznej realizowanych drogą elektroniczną, co stałoby w sprzeczności z przepisami ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne)\. Tego rodzaju ograniczeń nie powinny zwłaszcza nakładać przepisy aktu o randze niższej niż ustawa.

Podobną uwagę GIODO odniósł do wspomnianego projektu rozporządzenia Ministra Administracji i Cyfryzacji zmieniającego rozporządzenie w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej, który przewidywał rozwiązanie polegające na obligatoryjnym podawaniu numeru telefonu komórkowego jako jednego z elementów profilu zaufanego ePUAP. Generalny Inspektor wskazał, iż: „w przypadku akceptacji proponowanego przez projektodawcę rozwiązania będzie to oznaczało, że osoby nieposiadające telefonu komórkowego nie będą mogły utworzyć profilu zaufanego, co w znaczący sposób ogranicza możliwość dostępu do profilu zaufanego ePUAP, jak również

ogranicza możliwość autoryzacji (…). W opinii Generalnego Inspektora, sposób autoryzacji powinien następować – według wyboru użytkownika – na adres poczty elektronicznej lub na numer telefonu komórkowego".

Oba rozporządzenia zostały przyjęte **bez uwzględnienia uwag** Generalnego Inspektora Ochrony Danych Osobowych.

GIODO opiniował również projekt ustawy o zmianie ustawy – **Prawo o ruchu drogowym**[145] (etap prac sejmowych, podkomisja nadzwyczajna do rozpatrzenia rządowego projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw (druk nr 3525). Projekt ustawy przewidywał dostęp zakładów ubezpieczeń społecznych, będących spółkami prawa handlowego do danych zgromadzonych w centralnym rejestrze kierowców zarówno w trybie wnioskowym, jak i drogą zdalną, w postaci nieograniczonego dostępu do tychże danych – po wyrażeniu przez ministra właściwego do spraw wewnętrznych zgody, w drodze decyzji, na udostępnienie ich zakładom ubezpieczeń albo ich jednostkom organizacyjnym - bez konieczności składania pisemnego wniosku o taki dostęp. W tym kontekście pamiętać należy, iż danymi osobowymi zgromadzonymi w centralnej ewidencji kierowców są również dane podlegające szczególnej ochronie w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, to jest dane np. o osobach posiadających lub którym cofnięto uprawnienia do kierowania pojazdami silnikowymi, tramwajami lub motorowerami czy też dane o osobach nieposiadających uprawnień, w stosunku do których orzeczono środek karny w postaci zakazu prowadzenia. Generalny Inspektor Ochrony Danych Osobowych był przeciwny uprzywilejowaniu jednego z przedstawicieli komercyjnej grupy podmiotów (zakładów ubezpieczeń) w zakresie tego dostępu. Spółki te bowiem prowadzą swoją działalność celem przynoszenia określonych zysków, a informacje pozyskane z rejestru finansowanego ze środków publicznych mają dla nich wymierną wartość rynkową.

Sprzeciw GIODO wzbudził również zapis, zgodnie z którym minister do spraw wewnętrznych miałby prawo do udostępnienia danych zgromadzonych w centralnej ewidencji kierowców innym podmiotom, niż wymienione w przepisach projektowanej ustawy, w tym osobom fizycznym, osobom prawnym lub jednostkom organizacyjnym nieposiadającym osobowości prawnej, jeżeli wykażą swój uzasadniony interes. Organowi do spraw ochrony danych osobowych nie jest znana przesłanka „uzasadnionego interesu" jako podstawa dostępu do danych osobowych podlegających szczególnej ochronie w rozumieniu art. 27 ust. 1 ustawy

[145] DOLiS-033-283/15

o ochronie danych osobowych innym podmiotom – w tym osobom fizycznym, prawnym lub jednostkom organizacyjnym nieposiadającym osobowości prawnej. Wskazać należy, iż w obowiązującej ustawie – Prawo o ruchu drogowym, przesłanką udostępnienia przez ministra właściwego do spraw wewnętrznych danych zgromadzonych w centralnej ewidencji kierowców innym podmiotom, niż wymienione w przepisach tejże ustawy, w tym osobom fizycznym, osobom prawnym lub jednostkom organizacyjnym nieposiadającym osobowości prawnej, na ich pisemny wniosek, jest wykazanie przez te podmioty uzasadnionego interesu prawnego. Jeśli obowiązujące przepisy zapewniają wyższy poziom ochrony danych osobowych, w tym danych szczególnie chronionych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, niż przepisy projektowane, to wyjaśnienia oraz racjonalnego uzasadnienia wymaga powód, dla którego obniża się poziom ochrony danych osobowych z „uzasadnionego interesu prawnego" do „uzasadnionego interesu". Uwaga kwestionująca projektowany tryb udostępniania danych na umotywowany wniosek zainteresowanego podmiotu dotyczyła również przypadku udostępniania danych zgromadzonych w centralnej ewidencji posiadaczy kart parkingowych W tym przypadku nie było bowiem jasne jaką kategorię podmiotów stanowi „zainteresowany podmiot", a z analizy art. 100k ust. 2 i 3 projektowanej ustawy wynikało, iż „zainteresowane podmioty" wymieniane w ust. 2 nie były tożsame z „podmiotami, o których mowa w ust. 1" – to jest Policją, Inspekcją Transportu Drogowego, Żandarmerią Wojskową, Strażą Graniczną, starostą, strażami gminnymi oraz powiatowym zespołem do spraw orzekania o niepełnosprawności, czyli organami publicznymi, uprawnionymi do dostępu do tychże danych.

Akceptacji Generalnego Inspektora Ochrony Danych Osobowych nie zyskało również rozwiązanie przewidziane w art. 1 pkt 14 projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw dotyczące dodawanego do ustawy – Prawo o ruchu drogowym artykułu, zgodnie z którym danych zgromadzonych w centralnej ewidencji kierowców nie usuwa się, z wyłączeniem danych, o których mowa w art. 100aa ust. 4 pkt 12 i 13, które podlegają usunięciu z centralnej ewidencji kierowców na zasadach określonych w art. 98 ust. 5 i 6 ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2015 r. poz. 155, z późn. zm.). O ile do konstrukcji przepisu regulującego tryb usuwania z centralnej ewidencji kierowców danych, o których mowa w art. 100aa ust. 4 pkt 12 (to jest danych o wykroczeniach lub przestępstwach stanowiących naruszenia przepisów ruchu drogowego i przypisanych im punktach) organ do spraw ochrony danych osobowych uwag nie zgłaszał, o tyle dyspozycja art. 96 ust. 5 i 6 ustawy o kierujących pojazdami nie zapewnia regulacji

skutkującej usunięciem z centralnej ewidencji kierowców danych o kierowaniu pojazdami w stanie nietrzeźwości, w stanie po użyciu alkoholu lub środka działającego podobnie do alkoholu - art. 100aa ust. 4 pkt 13 projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw. Biorąc pod uwagę, iż informacje o kierowaniu pojazdem w stanie nietrzeźwości, w stanie po użyciu alkoholu lub środka działającego podobnie do alkoholu są informacjami potwierdzającymi fakt popełnienia przestępstwa lub wykroczenia przez kierowcę lub osobę posiadającą uprawnienia do kierowania tramwajem oraz stanowią kategorię danych podlegających szczególnej ochronie w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych, Generalny Inspektor Ochrony Danych Osobowych wskazał, iż należy przewidzieć oddzielny tryb regulujący usuwanie tego rodzaju danych z centralnego rejestru kierowców.

Do projektu ustawy nie dołączono również projektów podstawowych aktów wykonawczych, których brak stanowił ryzyko naruszenia przepisów dotyczących zasad ochrony danych osobowych ze względu na materię delegowanej regulacji. Taka wątpliwość zachodziła np. w przypadku wydania przez ministra właściwego do spraw wewnętrznych *szczegółowego katalogu gromadzonych w centralnej ewidencji kierowców danych*, jako że informacja o rodzajach danych gromadzonych w centralnej ewidencji kierowców stanowiłaby materiał porównawczy umożliwiający ocenę zasadności pozyskiwania określonych kategorii danych. Ustawa nowelizująca została uchwalona dnia 24 lipca 2015 r., a tekst nowelizacji został opublikowany w Dzienniku Ustaw pod poz. 1273.

Generalny Inspektor Ochrony Danych Osobowych zgłosił również swoje stanowisko do **ustawy o zmianie ustawy o transporcie drogowym**[146]**.** Zgodnie z proponowanym rozwiązaniem, w celu realizacji zadań określonych w art. 50 ustawy o transporcie drogowym, Inspekcja Transportu Drogowego może, w drodze teletransmisji danych, korzystać z bezpośredniego dostępu do danych zgromadzonych w Krajowym Rejestrze Karnym. Wskazać należy, iż ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2012 r. poz. 654 z późn. zm.) w art. 19 ust. 1 i 1a określa podmioty, którym udostępnia się dane o osobach oraz o podmiotach zbiorowych, zaś zgodnie z dyspozycją ust. 1b powołanego artykułu, zapytania i wnioski, o których mowa w ust. 1 i 1a, mogą być składane pisemnie albo za pośrednictwem systemu teleinformatycznego. Tryb udzielania informacji o osobach i informacji o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym

[146] DOLiS-033-66/15

Rejestrze Karnym oraz z rejestru karnego państwa obcego, określa rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2014 r. w sprawie trybu udzielania z Krajowego Rejestru Karnego informacji o osobach oraz o podmiotach zbiorowych za pośrednictwem systemu teleinformatycznego (Dz. U. poz. 841).

W tym kontekście wskazać również należy, iż zgodnie z art. 8 ust. 5 dyrektywy 95/46/WE Parlamentu i Rady 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie swobodnego przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, str. 31 z późn. zm.), przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane jedynie pod kontrolą władz publicznych, lub też, jeżeli zgodnie z prawem krajowym ustanowiono określone środki zabezpieczające, z zachowaniem odstępstw, które Państwo Członkowskie może udzielić zgodnie z obowiązującymi przepisami prawa krajowego, zapewniając zachowanie odpowiednich zabezpieczeń. Jednak kompletny rejestr przestępstw kryminalnych może być prowadzony tylko pod kontrolą władzy publicznej. Dlatego też w opinii Generalnego Inspektora Ochrony Danych Osobowych – brak jest uzasadnienia dla udzielenia Inspekcji Transportu Drogowego niczym nieograniczonego dostępu do danych zgromadzonych w Krajowym Rejestrze Karnym. Organ do spraw ochrony danych osobowych nie zauważa różnicy między Inspekcją Transportu Drogowego a 20 innymi podmiotami (art. 6 ustawy o Krajowym Rejestrze Karnym), dla których zasady dostępu do danych określa ustawa o Krajowym Rejestrze Karnym. Tymczasem proponowane przez Projektodawcę w art. 67 ust. 3a ustawy o transporcie drogowym, dodawanym przez art. 1 pkt 9 projektu ustawy o zmianie ustawy o transporcie drogowym, rozwiązanie, z nieznanych Generalnemu Inspektorowi Ochrony Danych Osobowych powodów, przyznaje Inspekcji Transportu Drogowego szczególny status nieomal oznaczający współadministrowanie Krajowym Rejestrem Karnym. Z takim zaś rozwiązaniem Generalny Inspektor Ochrony Danych Osobowych nie mógł się zgodzić.

Wyżej zaprezentowanego stanowiska organu do spraw ochrony danych osobowych nie zmienił również fakt, iż przewidziano w projektowanym art. 67 ust. 3a (*in fine*) ustawy o transporcie drogowym konstrukcję prawną, zgodnie z którą zasady dostępu Inspekcji Transportu Drogowego do danych Krajowego Rejestru Karnego miałoby określać porozumienie zawarte między Ministrem Sprawiedliwości a Głównym Inspektorem Transportu Drogowego. W ocenie Generalnego Inspektora Ochrony Danych Osobowych kwestie dostępu do danych Krajowego Rejestru Karnego w sposób wyczerpujący regulują

przepisy ustawy o Krajowym Rejestrze Karnym oraz aktów wykonawczych do tej ustawy, a zatem zawieranie porozumienia odmiennie regulującego powyższe zasady należy uznać za błędne.

Kwestią wymagającą wyjaśnienia była również przewidziana w projektowanym art. 82c pkt 2 i art. 82d ust. 2 ustawy o transporcie drogowym – kwestia przekazywanie danych do i z ewidencji poważnych naruszeń i ewidencji osób, które zostały uznane za niezdolne do kierowania operacjami transportowymi (odpowiednio art. 82c pkt 2 i art. 82d ust. 2 ustawy o transporcie drogowym, dodawane przez art. 1 pkt 11 projektu ustawy o zmianie ustawy o transporcie drogowym), przez dyrektorów izb celnych. Organowi do spraw ochrony danych osobowych nie są znane ustawowe kompetencje dyrektorów izb celnych, które uzasadniałyby przekazywanie i pozyskiwanie przez nich ww. danych szczególnie chronionych. Dlatego Generalny Inspektor Ochrony Danych Osobowych wnosi o wyjaśnienie przedmiotowej kwestii i – ewentualne – usunięcie dyrektorów izb celnych z dyspozycji projektowanego art. 82c pkt 2 i art. 82d ust. 2 ustawy o transporcie drogowym. Organ do spraw ochrony danych osobowych zakwestionował również sposób przekazywania danych osobowych projektowany w tej ustawie. Zarówno w odniesieniu do danych przekazywanych do Krajowego Rejestru Elektronicznego Przedsiębiorców Transportu Drogowego, jak i udostępniania danych na wniosek. Projektodawca przewidział dwa tryby ich przekazywania i udostępniania – za pośrednictwem elektronicznej platformy usług administracji publicznej lub w inny sposób, środkami komunikacji elektronicznej. O ile kwestia przekazywania i udostępniania danych za pośrednictwem elektronicznej platformy usług administracji publicznej jest uregulowana w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 z późn. zm.), to już określenie „lub w inny sposób, środkami komunikacji elektronicznej" wzbudziło zaniepokojenie Generalnego Inspektora Ochrony Danych Osobowych. Wskazać należy, iż niektóre rodzaje danych przekazywane w tych trybach, jak liczba, kategoria i rodzaj poważnych naruszeń, o których mowa w art. 6 ust. 1 lit. b rozporządzenia Parlamentu Europejskiego i Rady (WE) 1071/2009 z dnia 21 października 2009 r. ustanawiającego wspólne zasady dotyczące warunków wykonywania zawodu przewoźnika drogowego i uchylającego dyrektywę Rady 96/26/WE (Dz. Urz. UE L 300 z 14.11.2009 str. 51 z późn. zm.), które doprowadziły do skazania lub nałożenia sankcji w ciągu ostatnich dwóch lat; imię i nazwisko osoby uznanej za niezdolną do kierowania operacjami transportowymi do czasu przywrócenia dobrej reputacji tej osoby oraz data i miejsce jej urodzenia, jak również przyczyna stwierdzenia niezdolności, stanowią dane

podlegające szczególnej ochronie zgodnie z dyspozycją art. 27 ust. 1 ustawy o ochronie danych osobowych. W ocenie organu do spraw ochrony danych osobowych bezpieczeństwa danych przekazywanych w takim trybie nie zapewnia bliżej nieokreślony „inny sposób", jak i nieokreślone środki komunikacji elektronicznej. Zgodnie z protokołem nr 39/2015 (RM-000-39/165) z posiedzenia Rady Ministrów w dniu 22 września 2015 r., Rada Ministrów po dyskusji, odroczyła bezterminowo rozpatrzenie dokumentu.

W odniesieniu do **projektu ustawy o zmianie ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz niektórych innych ustaw**[147], Generalny Inspektor Ochrony Danych Osobowych stwierdził, iż mając na względzie powołane w uzasadnieniu do nowelizacji opiniowanej ustawy przepisy Dyrektywy Parlamentu Europejskiego i Rady 2013/50/UE z dnia 22 października 2013 r., która to z kolei dyrektywa w zakresie przetwarzania danych osobowych odwołuje się w pkt 21 (dodany art. 28c ust. 2 – Wykonywanie uprawnień do nakładania kar) do przepisów dyrektywy 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, organ do spraw ochrony danych osobowych wskazał na konieczność uwzględniania przepisów tej dyrektywy w odniesieniu do jakości danych, przez co w tym przypadku należy rozumieć zasadę ograniczenia czasowego przetwarzania danych osobowych. Zgodnie z art. 6 ust. 1 litera e dyrektywy 95/46/WE, Państwa Członkowskie zapewniają, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Państwa Członkowskie ustanowią odpowiednie środki zabezpieczające dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych. Treść powyższego przepisu w polskim porządku prawnym została transponowana do art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych. W związku z powyższym organ do spraw ochrony danych osobowych zwrócił się do Ministra Finansów z prośbą o rozważenie dodania do treści proponowanej nowelizacji przepisu ograniczającego czas podawania do publicznej wiadomości (niezależnie od formy czy nośnika takiego komunikatu) treści rozstrzygnięcia oraz informacji o rodzaju i charakterze naruszenia, imienia i nazwiska osoby fizycznej lub firmy (nazwy) innego podmiotu, na który nałożona została

[147] DOLiS-033-23/15

sankcja, o której mowa w ust. 1 e lub 1 f (art. 1 pkt 30 lit. g dotycząca dodawanego do ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych art. 10a pkt 1) – w odniesieniu do publikacji danych osobowych takiej osoby. Projekt ustawy o zmianie ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz niektórych innych ustaw (druk nr 70) został połączony do rozpatrywania z projektem ustawy o zmianie ustawy o funduszach inwestycyjnych oraz niektórych innych ustaw (druk nr 69). W wyniku ww. działań w dniu 31 marca 2016 r. uchwalono ustawę o zmianie ustawy o funduszach inwestycyjnych oraz niektórych innych ustaw. W dacie przygotowywania niniejszego sprawozdania oczekiwała ona na publikację w Dzienniku Ustaw.

Stanowisko organu do spraw ochrony danych osobowych zostało również wzięte pod uwagę przez Sejm w odniesieniu do **poselskiego projektu ustawy o zmianie ustaw o Najwyższej Izbie Kontroli**[148] (druk nr 257). Zmiana ta miała na celu zapewnienie zgodności proponowanej regulacji z wyrokiem Trybunału Konstytucyjnego z dnia 20 stycznia 2015 r. (Sygn. akt K 39/12), zgodnie z którym art. 29 ust. 1 pkt 2 lit. i ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2012 r. poz. 82, 1529 i 1544) w zakresie, w jakim uprawniał upoważnionych przedstawicieli Najwyższej Izby Kontroli do przetwarzania danych ujawniających poglądy polityczne, przekonania religijne lub filozoficzne, jak również dane o kodzie genetycznym, nałogach lub życiu seksualnym, został uznany za niezgodny z art. 47 oraz art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej. Generalny Inspektor Ochrony Danych Osobowych przedstawił swoją opinię w odniesieniu do nowego brzmienia art. 29 ust. 1 pkt 2 lit. i ustawy o Najwyższej Izbie Kontroli. Ustawa została uchwalona w dniu 20 marca 2015 r. i opublikowana w Dzienniku Ustaw pod poz. 684.

Wskazać ponadto należy, iż Generalny Inspektor Ochrony Danych Osobowych brał również aktywny udział w opiniowaniu dokumentów kierowanych pod obrady Komitetu Rady Ministrów do Spraw Cyfryzacji. Przedmiotem jego stanowisk były w szczególności projekty[149]:

- **rozporządzenia Ministra Sprawiedliwości w sprawie minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania systemu teleinformatycznego, w którym Krajowa Rada Notarialna prowadzi listę notariuszy**

[148] DOLiS-033-197/12
[149] DOLiS-033-206/15

oraz zastępców notarialnych – projekt ww. rozporządzenia nie określał warunków, jakie ma ów system zapewniać, gdyż nie wskazano miejsca i formy zapisu uprawnień, które mają być przedmiotem weryfikacji w systemie oraz procedury weryfikacyjnej, której zadaniem będzie wykonywanie tych weryfikacji. W szczególności nie podano w jakiej formie zapisane mają być w systemie przedmiotowe uprawnienia, kto jest/będzie uprawniony do ich wprowadzania, czy sam fakt wpisania na listę notariuszy oznacza posiadanie przedmiotowych uprawnień, czy też uprawnienia te zapisane mają być w postaci określonej cechy. Brak jest również informacji o działaniach jakie powinny być wykonane w przypadku negatywnego wyniku weryfikacji, a w szczególności czy i jak wynik weryfikacji przekazywany jest do systemu teleinformatycznego obsługującego postępowanie sądowe wniosków o wpis w księdze wieczystej. W treści projektu nie ma informacji w jaki sposób system teleinformatyczny, za pomocą którego prowadzona jest lista notariuszy i zastępców notarialnych, ma zapewniać zarówno weryfikacje przechowywanych danych, jak i posiadanych uprawnień. Poza tym w projekcie rozporządzenia była mowa, że przedmiotowy system ma zapewnić weryfikacje danych osobowych i posiadanych uprawnień notariuszy i zastępców notarialnych dla/w składanych wniosków/ach o wpis do księgi wieczystej za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe wniosków o wpis w księdze notarialnej. W treści projektu była również mowa, że system umożliwia automatyczne obsłużenie zapytania pochodzącego z systemu teleinformatycznego obsługującego postępowania wieczystoksięgowe wszczynane na wniosek składany za pośrednictwem tego systemu. Na podstawie tego ostatniego stwierdzenia „automatyczne obsłużenie zapytania pochodzącego z systemu teleinformatycznego obsługującego postępowania wieczystoksięgowe wszczynane na wniosek składany za pośrednictwem tego systemu" można przypuszczać, że przedmiotowy system miał służyć również do składania przedmiotowych wniosków. Należy zatem funkcjonalność tę (pośrednictwo w składaniu wniosków) dodać do listy wymaganych funkcjonalności. Z treści projektu rozporządzenia wynikało również, że projektowany system stanowi rejestr danych osobowych notariuszy i zastępców notarialnych zawierający ich dane osobowe i informacje o uprawnieniach do wykonywania wpisów do księgi wieczystej. Dalej w § 2 ust. 2 mówi się że system umożliwia automatyczne obsłużenie zapytania pochodzącego z systemu teleinformatycznego obsługującego postępowanie wieczystoksięgowe składane za pośrednictwem tego systemu. Brak było jednak informacji na czym ma polegać przedmiotowa weryfikacja uprawnień, jak również o tym, w jaki sposób analizowane ma być zapytanie pochodzące z systemu teleinformatycznego obsługującego

postępowania wieczysto księgowe i w jaki sposób ma następować przedmiotowa weryfikacja oraz co ma być wynikiem tej weryfikacji. W treści rozporządzenia brak było również jasnego podziału zadań realizowanych przez dwa systemy, tj. system teleinformatyczny obsługujący postępowanie wieczystoksięgowe oraz system, w którym KRN prowadzi listę notariuszy. W rezultacie treść projektu rozporządzenia stała się nieczytelna i bez dodatkowych wyjaśnień nie jest możliwa jego jednoznaczna interpretacja, co uniemożliwia tym samym jego ocenę.

- **rozporządzenia Rady Ministrów w sprawie organizacji systemu gromadzącego i udostępniającego informacje i dane od przedsiębiorcy telekomunikacyjnego –** GIODO zwrócił tu uwagę na fakt, iż projekt rozporządzenia ma określać nie tylko organizację ww. systemu, ale również jego funkcjonowanie. Tymczasem jednym ze słabych punktów ww. rozporządzenia jest brak wymagań w zakresie posiadania aktualnej polityki zapewnienia ciągłości działania (Business Continuity Plan - BCP) oraz wytycznych w zakresie wykonywania okresowych testów tego planu. BCP zestawi zbiór dokumentów określających organizację i zasady postępowania w ramach działań stanowiących zaplanowane reagowanie na nieoczekiwane wystąpienie zakłóceń w działalności organizacji (systemu). Plan odtwarzania utraconych zasobów (z ang. – disaster recovery plan – DRP) jako część BCP, koncentruje się na przywróceniu zasobów po wystąpieniu awarii (katastrofy). Jednym z najważniejszych elementów związanych z zapewnieniem ciągłości działania jest testowanie oraz utrzymanie planu ciągłości działania, czego brakowało w przedstawionym projekcie.

- dokumentu **Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych** – GIODO wskazał, iż w rozdziale 2.4.2 opiniowanego dokumentu przyjęto, że „w przypadku realizacji zadań publicznych unikanie ryzyka, co do zasady, nie ma zastosowania". Stwierdzenie to w ocenie organu do spraw ochrony danych osobowych było zbyt daleko idące, gdyż wiele zadań może być realizowanych przy zastosowaniu różnych, często alternatywnych środków technicznych i/lub organizacyjnych. Taka sytuacja ma na przykład miejsce w przypadku realizacji zadania, jakim jest umożliwienie składania rozliczeń podatkowych drogą elektroniczną - wówczas można przyjąć dwa alternatywne rozwiązania w zakresie podpisu elektronicznego, jakimi są: 1) podpis, przy użyciu certyfikatu lub Profilu Zaufanego lub 2) podpis polegający na dołączeniu do dokumentu informacji stanowiącej kwotę rozliczenia z poprzedniego roku. Przy takim rozwiązaniu zmniejszenie ryzyka złożenia fałszywego rozliczenia poprzez rezygnację z tej drugiej metody podpisu elektronicznego, tj. podpisu stanowiącego dołączenie

do dokumentu informacji z rozliczenia za poprzedni rok, byłoby przykładem unikania ryzyka. Nie oznacza to jednak, że podmioty zobowiązane do składania takich rozliczeń pozbawione byłyby możliwości rozliczeń drogą elektroniczną, gdyż rezygnacja dotyczyłaby jednej z dwóch, alternatywnych środków. Niezależnie od powyższego organ do spraw ochrony danych osobowych wskazał, iż Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych będzie stanowić istotną pomoc dla osób zajmujących się oceną ryzyka, a zastosowanie rozwiązań przyjętych w dokumencie przyczyni się do tego, że składane corocznie informacje do Ministra Administracji i Cyfryzacji dotyczące oceny ryzyk przez poszczególne podmioty będą porównywalne.

Generalny Inspektor uczestniczył także w pracach rządowych oraz parlamentarnych dot. projektu ustawy – Prawo o zgromadzeniach[150]. W ich toku kwestionowano potrzebę przedstawiania numeru PESEL albo rodzaju i numeru dokumentu tożsamości przez wnioskodawcę – organizatora zgromadzenia. Także rozszerzenie zakresu danych podawanych we wniosku stanowić może niebezpieczny precedens tworzenia szczególnej i wymagającej przetwarzania szerszego zakresu danych osobowych, metody składania pism do organu administracji publicznej. Przyjęcie takiego rozwiązania było krytykowane jako odejście od ogólnej normy art. 63 § 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjne (Dz. U. z 2013 r. poz. 267 z późn. zm.). W opinii Generalnego Inspektora zakres danych osobowych ujęty w tym przepisie jest wystarczający do zidentyfikowania nadawcy pisma w stopniu niezbędnym do prowadzenia postępowań administracyjnych i komunikowania się organu z interesantem. Wątpliwość budziło także wymaganie przedstawienia numeru telefonu oraz adresu poczty elektronicznej od wszystkich wnioskodawców, nie zaś umożliwienie tym osobom podania takich informacji na zasadzie dobrowolności.

W opinii Generalnego Inspektora nieuzasadnionym było także udostępnianie decyzji dotyczących zgromadzeń z podaniem szerokiego zakresu danych osobowych wnioskodawcy w Biuletynie Informacji Publicznej przez proponowany okres 3 miesięcy od dnia ich wydania. Publikacja decyzji na powszechnie dostępnej stronie internetowej stanowić może przetwarzanie danych wrażliwych w rozumieniu art. 27 ustawy o ochronie danych osobowych. Wątpliwość rodziło także kierowanie takiej decyzji do wszystkich użytkowników

[150] DOLiS-033-119/15

właściwego BIP, którzy w żadnym wypadku nie są uczestnikami postępowania i nie mają interesu w zapoznaniu się ze szczegółami decyzji, w tym danymi osobowymi wnioskodawcy.

Mimo aktywnego udziału przedstawicieli Generalnego Inspektora w procesie legislacyjnym w rządzie oraz parlamencie, **uwagi nie zostały wzięte pod uwagę** w ogłoszonej ustawie**.**

W zakresie uwag do projektu **ustawy o prekursorach materiałów wybuchowych podlegających ograniczeniom**[151] organ ds. ochrony danych postulował uporządkowanie katalogu przetwarzanych w systemie zgłaszania podejrzanych transakcji danych w taki sposób, by uniknąć przetwarzania danych nadmiarowych. Wątpliwość Generalnego Inspektora budził także zakres podmiotów, którym dane lub informacje zgromadzone w w/w systemie miały być udostępniane, ujęty w art. 11 projektu. Projekt w swojej pierwotnej wersji nie zawierał uregulowania w zakresie sposobu udostępniania informacji podmiotom określonym w art. 11. Organ podnosił, iż powinno to się dziać poprzez tryb wnioskowy, a nie bezpośredni dostęp do bazy danych. Uwagę zwracał także brak regulacji dotyczącej retencji danych i informacji zebranych w systemie. Generalny Inspektor postulował ograniczenie tego okresu do dwóch lat od daty zgłoszenia. Minister Gospodarki w toku prac rządowych przyjął większość uwag organu ds. ochrony danych osobowych. Prace legislacyjne nad tym projektem mogą być uznane za wzorcowy przykład współpracy pomiędzy organami państwa celem zapewniania bezpieczeństwa publicznego w poszanowaniu prawa jednostki do prywatności i ochrony danych osobowych.

Odnosząc się do projektu **ustawy o zmianie ustawy kodeks postępowania cywilnego oraz niektórych innych ustaw w związku ze wspieraniem polubownych metod rozwiązywania sporów**[152]**,** Generalny Inspektor oponował przeciw określeniu katalogu przetwarzanych danych mediatorów w akcie wykonawczym do ustawy. W opinii organu ds. ochrony danych osobowych niezbędne było uregulowanie pozostałych zasad, tak by w tekście rozporządzenia miało jedynie miejsce doprecyzowanie norm szerzej ujętych w tekście przyszłej ustawy. Warunki i tryb wpisywania oraz skreślania z listy stałych mediatorów, jako mające wpływ na prawa i obowiązki osób, powinny zostać ujęte w akcie rangi ustawowej. Wzór formularza wniosku o wpis na listę mógłby zostać następnie przygotowany przez Ministra Sprawiedliwości w oparciu o przepisy ustawy, które określać powinny m.in. zakres przetwarzanych danych osobowych oraz procedury składania wniosków. Generalny Inspektor

[151] DOLiS-033-226/15
[152] DOLiS-033-56/15 oraz DOLiS-033-236/15.

był także przeciwny wymaganiu podawania przez strony postępowania sądowego i ich pełnomocników, informacji o numerze telefonu i adresie poczty elektronicznej. W przepisach powinien być wskazany zamknięty katalog danych kontaktowych, które mają na celu umożliwienie sprawnego kontaktu pomiędzy mediatorem a stronami postępowania. Ich zakres powinien obejmować jedynie dane niezbędne. Na zasadzie fakultatywnej można podać adres poczty elektronicznej czy numer telefonu, o ile podmiot je posiada. W przeciwnym razie mogło dojść do sytuacji, w której sądy rozszerzałyby katalog danych wymaganych od stron postępowania i ich pełnomocników albo zobowiązywałyby te podmioty do przedstawienia takich danych w celu skutecznego prowadzenia postępowania procesowego. Sugerowane także projektodawcy rozważenie, czy niezbędnym jest podawanie numeru PESEL w sytuacji, gdy identyfikacja mediatora możliwa jest na podstawie daty urodzenia, która miała być podawana w razie braku numeru PESEL. W opinii Generalnego Inspektora połączenie takich danych jak data urodzenia oraz imienia i nazwiska jest wystarczające do celu dokonania identyfikacji osoby mediatora. Proponowano także ograniczenie informacji dotyczących wykształcenia mediatora i przebytego szkolenia jedynie do takich, które miałyby związek z wykonywaniem obowiązków mediatora. Było to w szczególności zasadne w obliczu propozycji brzmienia art. 183² § 3a pkt 1 K.p.c., zgodnie z którą mediator posiada wiedzę i umiejętności w zakresie prowadzenia mediacji.

Szczególną uwagę organ poświęcił problemowi wyraźnego określenia ról podmiotów zaangażowanych w projekt centralnej listy mediatorów. Zgodnie z brzmieniem propozycji Minister Sprawiedliwości miał być odpowiedzialny za administrowanie i udostępnianie listy w systemie teleinformatycznym. Natomiast prezesi sądów okręgowych mieli prowadzić na niej listy mediatorów stałych oraz osób prowadzących mediację zgodnie z przepisami o postępowaniu w sprawach nieletnich oraz K.p.k. dla obszaru właściwości danego sądu okręgowego. Generalny Inspektor zwrócił uwagę, iż w takiej sytuacji prezesi sądów okręgowych występowaliby w roli administratorów danych list dla okręgu sądowego, a Minister Sprawiedliwości mógł występować w roli administratora danych dla centralnej listy w skali kraju. W związku z powyższym konieczne było ustalenie zakresu odpowiedzialności i rzeczywistego wpływu na treść danych wprowadzanych do centralnej listy mediatorów. Przyznanie Ministrowi Sprawiedliwości statusu administratora danych w odniesieniu do danych mediatorów (w szerokim rozumieniu tego pojęcia), zawartych w centralnym systemie teleinformatycznym, implikować mogło po jego stronie konieczność wypełniania, określonych w projektowanej ustawie, obowiązków administratora danych (np. obowiązek

zapewnienia merytorycznej poprawności przetwarzanych danych – art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych). Tym samym Minister Sprawiedliwości, w świetle przepisów ustawy o ochronie danych osobowych, jako administrator danych byłby nie tylko uprawniony, ale wręcz zobowiązany do wprowadzania zmian do danych osobowych zebranych przez sądy przy rozpoznawaniu spraw. W ocenie Generalnego Inspektora dla realizacji – określonych w projekcie – zadań Ministra Sprawiedliwości związanych z informatyzacją sądownictwa zupełnie wystarczające byłoby przyznanie temu organowi statusu administratora systemu teleinformatycznego służącego do obsługi listy mediatorów i o podobną merytoryczną zmianę we wcześniejszych projektach organ do spraw ochrony danych osobowych zabiegał. W projektowanym art. 175b § 4 i 5 wskazano, iż Minister Sprawiedliwości jest uprawniony do udostępniania sądom oraz innym podmiotom aktualnych informacji z listy. Budzi to wątpliwości z dwóch przyczyn. Po pierwsze trudno jest udostępniać sądom dane, którymi prezesi sądów okręgowych już dysponują, jako że to oni uprzednio wprowadzili te dane do systemu. Po drugie nie określono zamkniętego katalogu podmiotów, którym Minister Sprawiedliwości będzie udostępniał informacje określone w § 3 pkt 1 i 3-7. Organ prosił projektodawcę o wyjaśnienie, czy jego intencją było, aby centralna lista była dostępna powszechnie za pośrednictwem publicznych sieci elektronicznych, czy też nie. W przypadku gdy centralna lista miałaby być publicznie dostępna, Generalny Inspektor zgłaszałby zastrzeżenia do upowszechniania tak szerokiego - jak zaproponowany - katalogu danych mediatorów, co mogło naruszać ich uzasadnione interesy.

Większość z uwag Generalnego Inspektora Ochrony Danych Osobowych została przyjęta albo wyjaśniona przez projektodawcę, co pozwoliło na przygotowanie projektu zgodnego z zasadami ochrony danych osobowych. Warto podkreślić, iż procedowanie tego projektu było również przykładem wzorowej współpracy przedstawicieli Ministerstwa Gospodarki oraz Generalnego Inspektora.

Do projektów **ustawy Kodeks budowlany oraz ustawy – Przepisy wprowadzające Kodeks budowlany**[153] Generalny Inspektor Ochrony Danych Osobowych zgłosił następujące uwagi. Projektowany art. 21 Kodeksu zawierał regulację rejestrów wymienionych w art. 21 § 1 pkt 1. Jednocześnie w ust. 2-6 wskazano zakres przetwarzanych i udostępniania danych oraz metody prowadzenia rejestrów. **Jednakże nie wskazano okresów retencji danych.** To na administratorze spoczywa obowiązek przechowywania danych w postaci umożliwiającej

[153] DOLiS-033-231/15

identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania. W związku z tym **powinny zostać przewidziane mechanizmy usuwania wpisów z rejestru**, które mogą z wielu przyczyn stać się nieaktualne oraz powinny być usuwane po ustaniu celu przetwarzania (np. archiwizowane, jeżeli zachodzi taka konieczność). Dotyczy to m.in. zatarcia kary ujętego w art. 252 Kodeksu. W takim przypadku, w publicznie dostępnej części rejestru, o którym mowa, nie powinna figurować żadna informacja o ukaraniu, podobnie jak ma to miejsce w przypadku Krajowego Rejestru Karnego. Analogiczną uwagę należało zgłosić do art. 18 pkt 5 Przepisów wprowadzających, który zawierał regulację rejestrów osób posiadających uprawnienia budowlane oraz osób ukaranych. Informacje o posiadanych uprawnieniach i nałożonych karach powinny być aktualizowane bądź usuwane, gdy ustał cel przetwarzania.

Projektowany art. 109 § 2 Kodeksu zawierał upoważnienie dla inwestora do wpisania do dziennika budowy danych kierownika budowy, projektanta i inspektora. Jednakże nie wskazano, jakie dane są wpisywane. Generalny Inspektor postulował, aby były to jedynie podstawowe dane identyfikacyjne, takie jak imię i nazwisko i numer uprawnień zawodowych, o których mowa np. w art. 21 § 4 lit. g Kodeksu. Także w przypadku § 5, który zawierał upoważnienie do wydania rozporządzenia m.in. w zakresie wzoru tablicy informacyjnej, postulowano wskazanie zakresu danych umieszczanych na tablicy. Dotychczasowe rozporządzenie[154] zawierało regulację zakresu danych osobowych, co w opinii Generalnego Inspektora wykraczało poza istniejącą oraz proponowaną w projekcie treść upoważnienia.

Korzystając z możliwości wpłynięcia na brzmienie nowego Kodeksu budowlanego Generalny Inspektor zwracał uwagę na kwestie, które rodzą wątpliwości podmiotów bezpośrednio stosujących postanowienia Prawa budowlanego[155] w zakresie przetwarzania danych osobowych. **Otrzymywane przez organ ds. ochrony danych osobowych sygnały wskazywały, iż istnieje konieczność doprecyzowania zakresu uprawnień kierownika budowy**. Zgodnie z ówczesnym brzmieniem art. 22 pkt 3d Prawa budowlanego, obowiązkiem kierownika budowy jest podejmowanie niezbędnych działań uniemożliwiających wstęp na budowę osobom nieupoważnionym. Generalny Inspektor stoi na stanowisku, iż przepis ten dawał uprawnienie do kontrolowania, kto uzyskuje wstęp na teren budowy oraz czy osoby te posiadają odpowiednie uprawnienia do wykonywania prac. Wiąże się to niejednokrotnie z

[154] Rozporządzenie Ministra Infrastruktury z dnia 26 czerwca 2002 r. w sprawie dziennika budowy, montażu i rozbiórki, tablicy informacyjnej oraz ogłoszenia zawierającego dane dotyczące bezpieczeństwa pracy i ochrony zdrowia, Dz. U. z 2002 r. Nr 108 poz. 953 z późn. zm.

[155] Ustawa z dnia 7 lipca 1994 r. Prawo budowlane, Dz. U. z 2013 r. poz. 1409 z późn. zm.

konieczności weryfikowania tożsamości pracowników budowy. W projekcie Kodeksu brak było takiego postanowienia. Jednocześnie kierownik budowy ma obowiązek kierowania robotami zgodnie z m.in. przepisami prawa, w tym także dotyczącymi bezpieczeństwa i ochrony zdrowia (art. 62 § 2 pkt 1 Kodeksu). Sygnały wpływające do Biura GIODO wskazywały, iż kierownicy budów mogą mieć trudności z uniemożliwianiem wstępu osobom nieupoważnionym, gdyż podwykonawcy powołują się na szeroko rozumianą ochronę danych osobowych i odmawiają przedstawiania informacji o pracownikach kierowanych na teren budowy i ich uprawnieniach. Należy przypomnieć, że za dopuszczenie do pracy osoby bez uprawnień odpowiedzialność ponosi kierownik budowy. W związku z tym istnieje konieczność umożliwienia tej osobie weryfikacji tożsamości i uprawnień w/w osób zgodnie z zasadami ochrony danych osobowych. Wprowadzenie jasnego przepisu w tym zakresie odpowiadałoby stworzeniu podstawy prawnej do przetwarzania danych w rozumieniu art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych. Ułatwiłoby to administratorom danych (w tym wypadku podmiotom prowadzącym prace budowlane i wyznaczającym m.in. kierownika budowy) przetwarzanie danych w tym niezbędnym do prawidłowego prowadzenia prac zakresie. Należy także pamiętać, iż w opisanej wyżej sytuacji może dochodzić do przetwarzania przez kierownika budowy tzw. danych wrażliwych w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych – np. zaświadczeń, czy informacji o braku przeciwwskazań zdrowotnych do pracy. Zgodnie z art. 27 ust. 2 pkt 2 w/w ustawy konieczna jest regulacja na poziomie ustawowym, która stwarza gwarancje ochrony takich danych, by możliwym było ich przetwarzanie. Także sposób przetwarzania w celu weryfikacji osób uzyskujących dostęp do terenu budowy powinien zostać wskazany. Generalny Inspektor postulował wprowadzenie takiej regulacji do projektu i był gotów wesprzeć projektodawcę w tym zakresie.

Ostatecznie projekt nie wyszedł poza etap uzgodnień międzyresortowych oraz konsultacji, w związku z czym stanowisko organu ds. ochrony danych osobowych pozostaje aktualne.

Opiniując **rządowy projekt ustawy o zmianie ustawy o świadczeniach rodzinnych oraz niektórych innych ustaw**[156], Generalny Inspektor Ochrony Danych Osobowych przypominał, iż odniesienia do ustawy o ochronie danych osobowych są zbędne, gdyż jako akt ogólny ma on zastosowanie, niezależnie od odesłań znajdujących się w omawianych

[156] DOLiS-033-237/15

przepisach projektu. Takie odesłania nie określały także w sposób wystarczający zasad przetwarzania danych przez ministra oraz upoważnione podmioty. To przepisach szczególnych powinny być określone wyczerpująco zasady przetwarzania danych przez administratora oraz podmioty, którym udostępniane są dane, w szczególności tryb pozyskiwania, udostępniania i przechowywania danych**.** Ogólne odesłanie do przepisów w/w ustawy mogły rodzić wątpliwości co do zasad przetwarzania danych mających zastosowanie.

Zaproponowane okresy retencji danych nie zostały w żaden sposób uzasadnione. Generalny Inspektor poddał w wątpliwość konieczność przechowywania informacji przez okres 10 lat od dnia zaprzestania udzielania świadczeń oraz 1 roku w przypadku, gdy świadczenie nie zostało przyznane oraz 10 lat od momentu ich udostępnienia uprawnionym organom. W ocenie organu ds. ochrony danych osobowych było to sprzeczne z podstawową **zasadą ograniczenia czasowego** przetwarzania danych, wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych. Nie było także jasnym, jakim celom miałoby służyć przechowywanie danych przez okres 10 lat po zaprzestaniu udzielania świadczeń oraz 1 roku w przypadku, gdy świadczenie nie zostało przyznane oraz 10 lat od momentu ich udostępnienia uprawnionym organom.

Wątpliwość budził dodawany art. 23b ust. 1 do ustawy o świadczeniach rodzinnych zobowiązujący do „**samodzielnego uzyskania** od organów podatkowych, organów emerytalno-rentowych oraz **z rejestrów publicznych, w drodze wymiany informacji w postaci elektronicznej** lub w drodze pisemnej (...) informacji i zaświadczeń**.** Wprowadzany przepis może stać się podstawą żądania właściwych, uprawnionych organów prowadzących postępowania w sprawie świadczeń rodzinnych oraz marszałka województwa do udostępnienia jego pracownikom bezpośredniego wglądu w dane przetwarzane w rejestrach publicznych, co może spowodować naruszenie ochrony danych, poprzez umożliwienie nieuprawnionego wglądu w dane, tj. wglądu w dane osób, które nie zwracały się do w/w organów o świadczenia rodzinne i wobec których nie toczy się żadne postępowanie w tych organach. Projektodawca powinien także zweryfikować, czy nie będzie to oznaczało konieczności zmiany przepisów dotyczących organów podatkowych, emerytalno-rentowych oraz prowadzących rejestry publiczne w zakresie katalogu podmiotów, którym mogą one udostępniać dane.

Wątpliwości budziło także pojęcie wymiany informacji, które mogą być zarówno pozyskiwane, jak i udostępniane w precyzyjnie określonych i niezbędnych sytuacjach. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących

zadania publiczne (t.j. Dz. U. z 2013 r. poz. 235 z późn. zm.) przewiduje tryb wnioskowy w dostępie do danych zgromadzonych w rejestrze publicznym, w zakresie niezbędnym do realizacji zadań jednostki, której dane są udostępniane. Jest to szczególnie istotne w obliczu przetwarzania danych wrażliwych związanych m.in. z pomocą rodzinie i osobom niepełnosprawnym. Także ewentualne dalsze wykorzystanie danych z rejestrów publicznych w innym celu niż realizacja zadań publicznych, musi być zgodne z zasadami ujętymi w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2014 r. poz. 782). Podstawową zasadą wypływającą z w/w aktów prawnych jest zakaz wykorzystania informacji dla innych celów, niż ustalone we właściwych przepisach.

W art. 3 pkt 1 projektu zaproponowano także korzystanie przez zespoły ds. orzekania o niepełnosprawności z danych o kwalifikacjach i umiejętnościach zawodowych oraz doświadczeniu zawodowym, a także o posiadaniu statusu bezrobotnego i pobieraniu świadczeń z tym związanych, które pozostają w dyspozycji Zakładu Ubezpieczeń Społecznych oraz publicznych służb zatrudnienia. Generalny Inspektor wnosił o rozpatrzenie, czy dane takie są w istocie niezbędne do przeprowadzenia postępowania mającego na celu potwierdzenie stanu zdrowia osoby wnioskującej o ustalenie niepełnosprawności albo o ustalenie stopnia niepełnosprawności. Dopuszczenie przetwarzania takich danych wydawało się sprzeczne z **zasadą adekwatności danych**. Członkowie w/w zespołów nie potrzebują takich kategorii danych do stwierdzenia stanu zdrowia wnioskującego w zakresie jego niepełnosprawności. W obliczu propozycji przetwarzania takich danych w Elektronicznym Krajowym Systemie Monitoringu Orzekania o Niepełnosprawności (proponowany art. 6d ust. 4 pkt 1a ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, Dz. U. z 2011 r. Nr 127, poz. 721 z późn. zm.) możliwym będzie także pozyskiwanie tych danych przez podmioty wymienione w projektowanym art. 6d ust. 4a w/w ustawy – organy samorządu terytorialnego oraz jednostki organizacyjne pomocy społecznej. Rozwiązanie takie w zakresie przetwarzania danych dotyczących sfery zawodowej wnioskodawców wydawało się bezzasadne.

W art. 4 pkt 6 zaproponowano, by rejestr centralny zawierał zanonimizowane informacje związane z przyznawaniem i realizowaniem świadczeń pomocy społecznej (projektowany art. 23a ust. 1 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, Dz. U. z 2013 r. poz. 182 z późn. zm., zwana dalej ustawą o pomocy społecznej). Jednocześnie kolejny projektowany przepis (art. 23a ust. 2 w/w ustawy) określał katalog danych, które mają być przetwarzane w rejestrze centralnym. Takie dwukierunkowe podejście wydawało się nie do

pogodzenia i rodziło wewnętrzną niespójność w projekcie. Generalny Inspektor sugerował doprecyzowanie omawianego przepisu.

W zakresie propozycji ujętej w art. 4 pkt 8 lit. b Generalny Inspektor poddał pod rozwagę możliwość uzupełnienia postanowienia z ust. 5g poprzez wprowadzenie pouczenia o możliwości uzyskiwania dostępu i poprawiania błędnych danych osobowych przez osoby ujęte w kwestionariuszu. Także w ustępie 5h proponowano doprecyzowanie, iż wywiad nie może być zmieniony w zakresie danych pozyskanych od osoby w trakcie przeprowadzonego wywiadu, chyba że są one nieprawidłowe. Stanowiłoby to realizację **praw kontrolnych osoby**, której dane dotyczą uregulowanych w art. 32 ustawy o ochronie danych osobowych.

Dwukrotnie w ubiegłym roku Generalny Inspektor wnosił uwagi do **projektów rozporządzenia Ministra Sprawiedliwości – Regulamin urzędowania sądów powszechnych**[157]**.** Wobec przepisów projektu znajdujących się w rozdziale 4 „Wokandy sądowe" (§ 59-62) Generalny Inspektor stanowczo oponował przeciwko rozstrzyganiu w akcie wykonawczym 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 opozycji do stanowiska zajmowanego przez Ministerstwo Sprawiedliwości, Generalny Inspektor w korespondencji dotyczącej tego zagadnienia od dłuższego czasu i konsekwentnie podnosił, że **kwestia treści wokandy i sposobu jej udostępniania stanowi materię ustawową w kontekście norm konstytucyjnych oraz przepisów ustawy o ochronie danych osobowych.** Regulacja treści wokand sądowych z pewnością nie należy do zakresu spraw mieszczących się w delegacji zawartej w art. 41 § 1 Prawa o ustroju sądów powszechnych do wydania *Regulaminu urzędowania sądów powszechnych*. W ocenie Generalnego Inspektora kwestia treści wokand sądowych należy do problematyki związanej ze sprawowaniem wymiaru sprawiedliwości, ustrojową pozycją sądów i korzystaniem przez jednostki z konstytucyjnych wolności i praw, w tym prawa do prywatności. W przekonaniu organu istotne wątpliwości co do dopuszczalności regulowania w akcie wykonawczym należało zgłosić również w stosunku do wielu innych regulacji projektu dotyczących praw i wolności obywatelskich, nieprzewidzianych w zakresie delegacji ustawy upoważniającej. W konsekwencji uregulowanie tych kwestii w akcie wykonawczym oznacza wejście rozporządzenia w materię ustawową.

[157] DOLiS-033-163/15, DOLiS-033-575/15.

Wątpliwości pod kątem przekroczenia upoważnienia ustawowego budził również § 11 projektu dotyczący **publikacji na stronach internetowych sądów informacji o osobach pełniących funkcje prezesa, wiceprezesa, przewodniczących wydziałów i ich zastępców oraz kierowników sekcji, wizytatorów, członków kolegium danego sądu, dyrektora sądu i jego zastępcy, kierowników sekretariatów i kierowników oddziałów, koordynatora ds. mediacji, imion i nazwisk kierowników zespołu opiniodawczych.** Obok problemu bliżej niesprecyzowanego zakresu „informacji o osobach" wskazano, że udostępnianie informacji o „organach i osobach sprawujących w nich funkcje i ich kompetencjach", stanowi zgodnie z art. 6 ust. 1 pkt 2 d ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2014 r. poz. 782) informację podlegającą udostępnieniu na zasadach określonych w tej ustawie. Trybunał Konstytucyjny w swoim orzecznictwie dotyczącym relacji między ustawą a rozporządzeniem (np. w wyroku z 22 marca 2007 r. sygn. U 1/07)[158], podkreślał, że „(...) wzajemne relacje pomiędzy ustawą a rozporządzeniem oparte są zawsze na założeniu, że akt wykonawczy konkretyzuje przepisy ustawy. [Akt wykonawczy] wydany może być tylko w zakresie określonym w upoważnieniu, w jego granicach i w celu wykonania ustawy w zgodzie z normami konstytucyjnymi, a także z wszystkimi obowiązującymi ustawami. Z art. 92 Konstytucji wynika, że ustrojodawca miał wolę pełnego, podmiotowego i przedmiotowego określenia zakresu prawodawstwa podustawowego i w tym celu nałożony został na ustawodawcę zwykłego obowiązek precyzyjnego i szczegółowego sformułowania zakresu delegacji, a przez to także obowiązek organów upoważnionych do ścisłego jej wykonania. Akt wykonawczy jest tym samym ściśle związany z wolą ustawodawcy, wyrażoną w ustawowej delegacji".

Generalny Inspektor wskazał jednocześnie, że z projektu rozporządzenia Ministra Sprawiedliwości powinien ulec wykreśleniu § 89 dopuszczający nagrywanie rozmów telefonicznych kierowanych do sądu. Zasadnie należy założyć, że treść powyższych połączeń telefonicznych zawiera informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych. Uprawnienie prezesów sądów do zdecydowania o nagrywaniu rozmów telefonicznych może zatem prowadzić do gromadzenia i przechowywania danych osobowych i to danych wrażliwych w rozumieniu art. 27 ustawy o ochronie danych osobowych w zbyt szerokim zakresie. Należy mieć świadomość, że z

[158] OTK ZU nr 3/A/2007, poz. 29.

powyższym uprawnieniem wiąże się możliwość tworzenia zbiorów danych, które muszą być odpowiednio chronione w zależności od charakteru zebranych w nich danych osobowych.

W omawianym projekcie brakowało określenia nie tylko celów, ale i zasad „nagrywania rozmów", w tym gromadzenia, udostępniania nagrań, dalszego ich przechowywania, zapewnienia dostępu do danych osób, których informacje o charakterze osobowym dotyczą i ich zabezpieczenia przed niepowołanym dostępem oraz okresu retencji danych. Prezesom sądów pozostawiona została daleko idąca dowolność i swoboda w tym zakresie. Tak ogólnikowe regulacje są oczywiście niewystarczające i stanowią oczywiste zagrożenie dla praw i wolności jednostki. Zgodnie z art. 26 ust. 1 pkt 1 i 3 ustawy o ochronie danych osobowych administrator danych powinien zapewnić, by przetwarzane informacje (dane osobowe zwykłe i wrażliwe) były adek0watne do celów, w jakich są przetwarzane. Art. 32 ustawy o ochronie danych osobowych dotyczy praw do kontroli przetwarzania danych, które jej dotyczą. Zasady udostępniania nagrań rozmów telefonicznych powinny regulować także uprawnienia osób nagrywanych do dostępu, żądania usunięcia lub wniesienia sprzeciwu wobec przetwarzania ich danych.

Z analogicznych jak powyższe względów Generalny Inspektor Ochrony Danych Osobowych poddał pod rozwagę projektodawcy również inne projektowane rozwiązania. Jako przepisy mogące budzić istotne wątpliwości, czy nie powinny być przeniesione do aktu rangi ustawowej wskazano przepisy dotyczące: posiadania i okazywania dowodu osobistego lub innego dokumentu stwierdzającego tożsamość i odnotowywanie tego w protokole (§ 82 projektu), udostępniania informacji drogą elektroniczną przez strony, uczestników lub ich pełnomocników (§ 90 projektu), rozpoznawania wniosków o udostępnienie akt, zapisu dźwięku albo obrazu i dźwięku oraz wydanie kopii tego zapisu (§ 98 projektu), udostępniania danych o sprawie, treści protokołów oraz pism sądowych i procesowych za pomocą kont w systemie teleinformatycznym (§ 98, 100-104 projektu), ustalenia przez sąd rejestrowy danych identyfikacyjnych wpisywanej do Krajowego Rejestru Sądowego osoby (§ 170 projektu), uprawnienia sądu rejonowego do ustalania numeru PESEL dłużnika, a w razie braku takiej możliwości ujawniania w sentencji orzeczenia, poza imieniem i nazwiskiem dłużnika wpisywanego z urzędu do Rejestru Dłużników Niewypłacalnych, także datę i miejsce urodzenia, imiona rodziców, aktualny adres oraz serię i numer dokumentu tożsamości (§ 183), zapisanie danych osobowych pracownika lub ubezpieczonego (§ 186 projektu), udostępniania akt ksiąg wieczystych do wglądu notariuszom i innym osobom (§ 211 projektu), określania w orzeczeniach stanowiących podstawę wpisu w aktach stanu cywilnego oraz w protokołach

uznania ojcostwa danych osobowych stron (§ 218 projektu), udostępnianie i przesyłanie akt za pośrednictwem kont albo systemu teleinformatycznego (§ 266-267 projektu), wydawania zarządzeń o zgodzie na widzenie z tymczasowo aresztowanym (§ 311 i 312 projektu), zamieszczanie danych dotyczących zarzucanego czynu i dotychczasowej karalności osoby pozbawionej wolności oraz wskazywanie osób, z którymi nie powinien przebywać w czasie przewozu (§ 309 projektu), cenzurowania korespondencji osoby tymczasowo aresztowanej (§ 314 projektu), wydawania zgody na korzystanie przez tymczasowo aresztowanego z aparatu telefonicznego (§ 315 projektu), przesyłanie informacji o skazanych do administracji zakładu karnego lub aresztu śledczego (§ 318 projektu), wydawania zwalnianemu zaświadczenia potwierdzającego „najważniejsze dane personalne" w razie uchylenia tymczasowego aresztowania (§ 319 projektu), informowanie Straży Granicznej oraz organu paszportowego o zakazie opuszczania kraju i zatrzymaniu dokumentu paszportowego (§ 327 projektu), dokonywania wpisów, modyfikacji oraz usunięcia danych SIS (§ 331 projektu), udzielania informacji przez sądy przedstawicielowi krajowemu w Eurojust (§ 351).

Jednoznaczne brzmienie art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych wskazuje, że konieczne jest istnienie ustawowych podstaw prawnych dla przetwarzania danych np. o karalności. Konieczne jest zatem zezwolenie na takie przetwarzanie w przepisach ustawy, stwarzającej przy tym pełne gwarancje ochrony tych danych. 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.

Podkreślenia wymaga, że projektodawca konsekwentnie ignorował stanowisko organu ds. ochrony danych osobowych przedstawiane w 2015 r. oraz w uprzednich latach sprawozdawczych.

W odniesieniu do projektu **uchwały Rady Ministrów w sprawie Rządowego programu wspomagania w latach 2015 – 2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach – „Bezpieczna+"** oraz **rozporządzenia Rady Ministrów w sprawie szczegółowych warunków, form i trybu realizacji Rządowego programu wspomagania w latach 2015 – 2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki,**

wychowania i opieki w szkołach – „Bezpieczna+”[159]**,** Generalny Inspektor zgłaszał poparcie dla propozycji poprawiających bezpieczeństwo uczniów, nauczycieli i innych pracowników szkół. Jednocześnie koniecznym było podniesienie szczegółowych uwag w zakresie wprowadzania do szkół i innych placówek oświatowych monitoringu wizyjnego na podstawie przepisów aktu wykonawczego do ustawy z dnia 7 września 1991 r. o systemie oświaty Dz. U. z 2004 r. nr 256 poz. 2572, z późn. zm. Sugerowano projektodawcy, iż powinien odpowiedzieć na pytanie o **adekwatność wprowadzenia monitoringu wizyjnego do szkół** jako metody zapewniania bezpieczeństwa w szkole i czy inne, mniej inwazyjne rozwiązania nie przyniosłyby oczekiwanych efektów w zakresie zapewniania bezpieczeństwa.

W związku z tym wskazano na potrzebę przeprowadzenia **analizy potrzeb i celowości budowy systemu,** w której podmiot podejmujący decyzję o budowie lub rozbudowie systemu monitoringu zobowiązany byłby do przeprowadzenia prognozy skuteczności funkcjonowania systemu, analizy rozwiązań alternatywnych i specyfiki zagrożeń w danym rejonie, optymalnego rozmieszczenia kamer oraz ocenę wpływu projektowanego systemu na prywatność (tzw. *privacy impact assessment*). Przywołano projekt unijnego rozporządzenia o ochronie danych osobowych[160], zgodnie z którym takie oceny będą obowiązkowe w przypadku operacji przetwarzania stwarzających ryzyko dla ochrony praw i wolności podmiotów danych, takie jak m.in. prowadzenie monitoringu wizyjnego. Analizy te powinny także obejmować **zagadnienie przetwarzania danych innych osób**, które mogą znaleźć się na obszarze monitorowanym, gdyż z treści projektu Programu wynikało, że monitoringowi mają podlegać m.in. wejścia i otoczenie szkoły. W tych obszarach mogą znaleźć się osoby, które nie będą świadome, iż teren placówki objęty jest monitoringiem. Także wobec nich administrator danych, którym będzie kierownik jednostki, ma zobowiązania do: poinformowania o stosowaniu obserwacji, zapewnienia dostępu do danych tych osób dotyczących i ich zabezpieczenia przed niepowołanym dostępem. Oddzielną kwestią jest przetwarzanie przy pomocy kamer monitoringu danych nauczycieli i innych pracowników szkoły. Nie powinien on służyć do realizacji celu kontrolowania poczynań pracowników i uczniów, jako metoda nadmierna. Elektroniczny system nie powinien zastąpić bieżącego nadzoru, jaki przełożony może sprawować nad swoimi podwładnymi oraz nauczyciel nad uczniami.

[159] DOLiS-033-204/15

[160] Wniosek dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, COM(2012) 11, Dz. Urz. C 102 z dnia 5 kwietnia 2012 r. s. 24.

Podkreślano, że to na ustawodawcy spoczywa obowiązek ustalenia zasad gromadzenia i udostępniania nagrań, tak by uniknąć dowolności w tym zakresie, która może wystąpić, jeżeli szkołom pozostawiona byłaby daleko idąca swoboda, jak ma to miejsce obecnie. Ogólnikowe regulacje są w tym przypadku niewystarczające i wymagają daleko posuniętego doprecyzowania. Sygnały otrzymywane przez Biuro GIODO na temat nieuporządkowanego stosowania monitoringu wizyjnego, nie tylko w placówkach oświatowych, wskazują na możliwe negatywne konsekwencje. Obywatele poddani monitoringowi mogą odczuwać długotrwały dyskomfort psychiczny związany z postrzeganym przez nich znaczącym naruszeniem prywatności. Jednocześnie widoczne są tendencje do poszerzania zakresu monitoringu o nowe wymiary, jak chociażby możliwość stosowania, obok rejestracji obrazu, także nagrywania dźwięku, czyli podsłuchiwania rozmów. Powstaje pytanie, czy nawet najlepiej przygotowane i kompetentni pracownicy szkół będą w stanie w sposób wystarczający zapewnić ochronę praw użytkowników tych instytucji w obliczu braku określenia przez państwo jasnych reguł dozwolonego postępowania.

W związku z tym Generalny Inspektor przypomniał, iż każdorazowe wprowadzanie regulacji dotyczących monitoringu wizyjnego powinno podlegać ocenie zgodnie z **zasadą proporcjonalności ujętą w art. 31 ust. 3 Konstytucji.** Przytoczono także stanowisko Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Szerokie rozprzestrzenienie monitoringu w przestrzeni publicznej i prywatnej nie powinno w sposób nieuzasadniony ograniczać praw i wolności jednostki[161].

Krytyce poddano również brak jasnego uregulowania w zakresie **zasad pozyskiwania, gromadzenia i udostępniania nagrań,** który powinien zostać uzupełniony. Powinny one być adekwatne do zakładanych celów monitoringu. Tylko w takiej sytuacji możliwe będzie wprowadzanie monitoringu na prostych i klarownych zasadach. To umożliwiłoby administratorom spełnianie zobowiązań wobec osób obserwowanych do poszanowania ich prywatności i zapewniania bezpieczeństwa. Zasady udostępniania nagrań z monitoringu powinny regulować także uprawnienia osób obserwowanych do dostępu, żądania usunięcia lub wniesienia sprzeciwu wobec przetwarzania ich danych. Kwestie te są ściśle związane z respektowaniem jeszcze innego obowiązku, a mianowicie obowiązku informacyjnego. Właściwie ukształtowane zasady muszą być w sposób klarowny przekazywany osobom obserwowanym poprzez **realizację obowiązku informacyjnego**. Nie powinno być

[161] Opinia Grupy Roboczej art. 29 nr 4/2004 o przetwarzaniu danych osobowych przy pomocy wideomonitoringu z dnia 11 lutego 2004 r. 11750/02/EN WP89, s. 4.

możliwym zbieranie danych bez wiedzy tych osób. Realizacja obowiązku powinna się odbywać przez tablice informacyjne, piktogramy, wyraźne oznaczenie kamer oraz łatwo dostępne polityki prywatności, o czym organ ds. ochrony osobowych szeroko pisał w uwagach do projektu założeń do ustawy o monitoringu wizyjnym. Z uwagi na specyficzny charakter przetwarzania bez dodatkowej regulacji administratorzy danych mogą mieć trudności w realizacji obowiązków wynikających z ustawy o ochronie danych osobowych.

Projektodawca nie wskazał w żaden sposób, **jakie obszary na terenie szkoły mogą być obserwowane.** Koniecznym jest rozstrzygnięcie, czy ma się to odbywać także w klasach. Generalny Inspektor zalecił w tym obszarze daleko idącą ostrożność i przestrzegał przed pozostawianiem takich decyzji administratorom danych – dyrektorom i kierownikom placówek – ponieważ może to rodzić nieprawidłowości i negatywne konsekwencje, a przede wszystkim nie służyć założonym celom.

Generalny Inspektor zwrócił uwagę, iż konieczne jest uregulowanie **zasady ograniczenia czasowego przetwarzania danych** uzyskanych w toku pracy systemów monitoringu. Ma ona bezpośredni związek z okresem retencji danych. Nie powinno się pozostawiać administratorom swobody w zdefiniowaniu okresu retencji z perspektywy funkcjonowania poszczególnych systemów. Celem, który przyświeca projektodawcy miało być bezpieczeństwo użytkowników szkoły. W sierpniu 2014 r. (w toku prac nad ustawą o monitoringu wizyjnym) Generalny Inspektor sygnalizował, iż w niektórych państwach maksymalny okres przechowywania wynosi 72 godziny. Wydawało się zasadnym maksymalne ograniczenie okresu retencji, gdyż w szkołach mają być stosowane także inne metody zapewniania bezpieczeństwa. Ewentualne nagrania, które mogą być istotne dla wyjaśniania niepożądanych zdarzeń, mogą być zabezpieczane w okresie krótszym, gdyż sprawdzenie nagrań z systemu monitoringu będzie wykonywane w pierwszej kolejności. Nagrania nie powinny być także przechowywane dłużej dla innych, niż zapewnianie bezpieczeństwa celów. Retencja danych powinna być za każdym razem dostosowywana do celu realizowanego przez administratora. Nie powinno też dochodzić do gromadzenia nagrań na zapas.

W zakresie opisu technologii, które miałyby być wprowadzone do monitorowania przestrzeni, nie wskazano takich cech, jak jakość nagrania, dopuszczalność rejestracji dźwięku oraz czy oprogramowanie będzie umożliwiało analizę rejestrowanych obrazów (identyfikacja wizerunków, wykrywanie zachowań niepożądanych itp.). **Dopuszczenie takich rozwiązań byłoby wysoce dyskusyjne z punktu widzenia ochrony podmiotu danych i z**

tego powodu potrzebne jest precyzyjne ustalenie kryteriów technicznych. Bez takiego uregulowania może dochodzić do daleko idących różnic w systemach używanych w szkołach. Z uwagi na specyfikę technologii i ryzyk związanych z tą formą przetwarzania danych, warunki techniczne mogłyby być uregulowane na poziomie ustawy. Potrzebne byłoby także **uregulowanie zasad zabezpieczania wytworzonych nagrań przed dostępem osób nieupoważnionych.** W zależności od zastosowanych technologii przesyłu może to wiązać się ze stosowaniem szyfrowania transmisji bezprzewodowych albo zabezpieczenie połączeń między systemem zapisującym a kamerami.

Stanowisko organu ds. ochrony danych osobowych było konsekwentnie prezentowane na dalszych etapach procesu legislacyjnego (podczas obrad Komitetu Rady Ministrów ds. Cyfryzacji oraz Stałego Komitetu Rady Ministrów). W związku z przyjęciem uwag Generalnego Inspektora, Ministerstwo Edukacji Narodowej ograniczyło treść projektów do kwestii niezwiązanych z monitoringiem wizyjnym. W toku całego procesu zwracano także uwagę na brak postępów w pracach nad ustawą o monitoringu wizyjnym. Bez takiej regulacji niemożliwe jest prawidłowe funkcjonowanie systemów monitoringu wizyjnego w kraju, które realizowałoby jednocześnie interesy administratorów systemów jak i osób obserwowanych, których prawo do prywatności oraz ochrony danych osobowych musi być respektowane.

W 2015 roku zostały zakończone – zainicjowane w 2013 roku[162] i kontynuowane w 2014 roku[163] – prace legislacyjne dotyczące **ustawy z dnia 9 października 2015 roku o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**[164]. Jak było to już sygnalizowane w „Sprawozdaniu z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2014", autorzy tego projektu[165] zdecydowali o przeprowadzeniu kompleksowej nowelizacji przepisów ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia[166] oraz kilku innych ustaw dotyczących takich kwestii jak: prawa pacjenta, przetwarzanie danych medycznych, wykonywanie zawodów medycznych. Takie rozstrzygnięcie projektodawcy przesądziło o konieczności przeprowadzenia przez organ do

[162]Dokument *„Założenia do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw"*, DOLiS-033-465/13.

[163] DOLiS-033-340/14 – „Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2014" – str. 141–143.

[164] Dz. U. z 2015 r. poz. 1991 z późn. zm.

[165] DOLiS-033-340/14

[166] Dz. U. z 2015 r. poz. 636 z późn. zm.

spraw ochrony danych osobowych niezależnej oceny kilku zagadnień objętych przedmiotowym projektem.

I tak – w pierwszej w 2015 roku opinii do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (wersja z dnia 17.02.2015 r.)[167], Generalny Inspektor Ochrony Danych Osobowych zawarł następujące uwagi:

- w miejsce definicji pojęcia „certyfikat" zamieszczonej w art. 1 pkt 1 lit. a projektu z 17.02.2015 r., organ do spraw ochrony danych osobowych proponował własną definicję tego pojęcia w brzmieniu: „certyfikat – elektroniczne poświadczenie tożsamości systemu usługodawcy, wydane na wniosek usługodawcy, umożliwiające mu wymianę informacji z systemem, o którym mowa w art. 7";
- niezrozumiały dla Generalnego Inspektora Ochrony Danych Osobowych był – zawarty w art. 1 pkt 2 lit. b projektu z 17.02.2015 r. - postulat rozszerzenia sformułowanego w art. 4 ust. 3 ustawy o systemie informacji w ochronie zdrowia, katalogu danych osobowych usługobiorców przetwarzanych w systemie informacji w ochronie zdrowia o adres zameldowania w sytuacji, gdy zamiarem ustawodawcy było zniesienie obowiązku meldunkowego;
- tym samym zachodziła też potrzeba wprowadzenia stosownej zmiany w punktach 1 i 2 art. 15 ust. 5 ustawy o systemie informacji w ochronie zdrowia, w brzmieniu nadanym przez art. 1 pkt 11 lit. c projektu z 17.02.2015 r., polegającej na usunięciu obowiązku przekazywania przez ministra właściwego do spraw wewnętrznych do Centralnego Wykazu Usługobiorców, danej o adresie zameldowania usługobiorcy oraz zapewnienia stałego do niej dostępu;
- akceptując fakt przeniesienia do regulacji ustawowej (art. 11 ust. 4 pkt 13 ustawy o systemie informacji w ochronie zdrowia, dodawany przez art. 1 pkt 7 lit. b projektu z 17.02.2015 r.) przepisu nakazującego wskazanie podmiotu odpowiedzialnego za przechowywanie i udostępnianie dokumentacji medycznej, Generalny Inspektor Ochrony Danych Osobowych podnosił, iż w dalszym ciągu nie została w sposób prawidłowy uregulowana kwestia sposobu postępowania z dokumentacją medyczną po likwidacji podmiotu leczniczego albo zakończeniu działalności leczniczej przez lekarza lub pielęgniarkę, którzy wykonywali zawód w ramach praktyki zawodowej. Dotyczące tej kwestii odpowiednio - art. 106 ust. 3 pkt 10 a ustawy z dnia 15 kwietnia 2011 roku

[167] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 11 marca 2015 roku do Sekretarza Stanu w Ministerstwie Zdrowia, sygn. DOLiS-033-340/14/TG/19684/15.

o działalności leczniczej[168] i art. 106 ust. 4 pkt 8 a ustawy o działalności leczniczej - ograniczają się jedynie do nałożenia obowiązku wskazania we wniosku rejestracyjnym miejsca przechowywania dokumentacji medycznej w wyżej wskazanych przypadkach, pozostawiają jednak pełną dowolność przy wyborze tego miejsca oraz nie nadają organowi rejestrującemu kompetencji do weryfikowania prawidłowości wskazanego miejsca;

- wątpliwości budził także zapis w art. 14 a ust. 11 pkt 2 ustawy o systemie informacji w ochronie zdrowia, dodawanym przez art. 1 pkt 10 projektu z 17.02.2015 r. W powołanym przepisie znalazło się stwierdzenie, że warstwa elektroniczna Karty Specjalisty Medycznego zawiera dane: „służące do składania podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym;". Równocześnie w projekcie z 17.02.2015 r. brak jest informacji o podmiocie, który będzie pełnił funkcję urzędu certyfikującego;
- Generalny Inspektor Ochrony Danych Osobowych nie znajdował uzasadnienia dla przekazywania przez ministra właściwego do spraw wewnętrznych do Centralnego Wykazu Usługobiorców, danej o stanie cywilnym usługobiorcy (art. 15 ust. 5 pkt 1 - w zakresie lit. e w wersie drugim - ustawy o systemie informacji w ochronie zdrowia, w brzmieniu nadanym przez art. 1 pkt 11 lit. c projektu z 17.02.2015 r.). W opinii organu do spraw 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 z dnia 29 sierpnia 1997 roku o ochronie danych osobowych[169] – zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane;
- mając na uwadze, iż celem rozporządzenia wykonawczego wydawanego na podstawie delegacji z art. 31 ustawy o systemie informacji w ochronie zdrowia jest zapewnienie, aby systemy, o których mowa w artykułach: 27, 29 i 30 ustawy o systemie informacji w ochronie zdrowia zapewniały integralność przetwarzanych danych, w opinii Generalnego Inspektora Ochrony Danych Osobowych przedmiotowe rozporządzenie winno określać wymagania, jakie powinny spełniać te systemy (w tym ich funkcjonalności), nie zaś zawierać opis tych systemów. W tym stanie rzeczy organ do spraw ochrony danych

[168] Dz. U. z 2015 r. poz. 618 z późn. zm.
[169] Dz. U. z 2015 r. poz. 2135 z późn. zm.

osobowych wnosił o stosowną zmianę delegacji ustawowej zaproponowanej w art. 1 pkt 28 projektu z 17.02.2015 r.;

- w świetle – przedstawionych w art. 1 pkt 29 projektu z 17.02.2015 r. – unormowań dotyczących zgody usługobiorcy (jego przedstawiciela ustawowego lub osoby przez usługobiorcę upoważnionej), sprzeciwu oraz określenia zakresu dostępu do danych medycznych (nowe brzmienie art. 35 ustawy o systemie informacji w ochronie zdrowia) Generalny Inspektor Ochrony Danych Osobowych zwrócił się do projektodawcy o wyjaśnienie zasad funkcjonowania proponowanego systemu teleinformatycznego, a w szczególności kwestii sposobu wyrażania zgody (sprzeciwu) przez usługobiorcę (jego przedstawiciela ustawowego lub osobę przez niego upoważnioną), możliwości zmiany wcześniej podjętej decyzji, itd. Zagadnienie to jest tym bardziej istotne, jeśli zauważyć, że proponowany – w dodawanym przez art. 1 pkt 29 lit. d projektu z 17.02.2015 r. – system teleinformatyczny ma umożliwić składanie przez usługobiorcę (jego przedstawiciela ustawowego lub osobę przez niego upoważnioną) oświadczeń woli w postaci elektronicznej, co stanowić będzie odstępstwo od zasady z art. 27 ust. 2 pkt 1 ustawy o ochronie danych osobowych.
- w zakresie zmian do ustawy z dnia 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[170] dotyczących karty ubezpieczenia zdrowotnego, zwanej dalej „KUZ" (art. 49 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w brzmieniu nadanym przez art. 7 pkt 11 projektu z 17.02.2015 r.), organ do spraw ochrony danych osobowych wskazał, iż:
  a. w art. 49 ust 1 pkt 2 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w brzmieniu nadanym przez art. 7 pkt 11 projektu z 17.02.2015 r., użyto sformułowania: „[…] złożenie podpisu elektronicznego pod dokumentem elektronicznym." (w celu potwierdzenia wykonania świadczeń opieki zdrowotnej). Mając na uwadze definicję podpisu elektronicznego bardziej właściwym – w opinii Generalnego Inspektora Ochrony Danych Osobowych – jest sformułowanie: „złożenie podpisu elektronicznego" bez wskazywania czy podpis ma być **pod** dokumentem elektronicznym, czy **na** tym dokumencie,
  b. w art. 49 ust 4 pkt 2 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, w brzmieniu nadanym przez art. 7 pkt 11 projektu z

[170] Dz. U. z 2015 r. poz. 581 z późn. zm.

17.02.2015 r. zapisano, że warstwa elektroniczna KUZ zawiera dane: „służące do składania podpisu elektronicznego weryfikowanego przy pomocy ważnego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym […]". Tymczasem w przypadku Karty Specjalisty Medycznego użyto sformułowania: „przy pomocy ważnego kwalifikowanego certyfikatu […]" (patrz pkt V.). Wymagało zatem wyjaśnienia, czy ta rozbieżność jest skutkiem błędu projektodawcy, czy też działaniem celowym wskazującym na różny poziom wiarygodności tych dwóch certyfikatów.

- identyczną uwagę do zamieszczonej w pkt IX. lit. b. organ do spraw ochrony danych osobowych zgłosił do art. 49 a ust 7 pkt 2 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, dodawanego przez art. 7 pkt 12 projektu z 17.02.2015 r., regulującego zakres danych w warstwie elektronicznej Karty Specjalisty Administracyjnego;
- w związku z podjętą przez projektodawcę w nowelizowanej (art. 10 projektu z 17.02.2015 r.) ustawie z dnia 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta[171], próbą uregulowania dostępu do dokumentacji medycznej przez inne osoby aniżeli wykonujące zawód medyczny (art. 24 ust. 2 i 3 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 17.02.2015 r.), Generalny Inspektor Ochrony Danych Osobowych stanął na stanowisku, że zaproponowane rozwiązanie jest niewystarczające dla zapewnienia ochrony danych wrażliwych, jakimi są dane o stanie zdrowia. W opinii organu do spraw ochrony danych osobowych nie można uznać za poprawne i stwarzające pełne gwarancje ochrony danych szczególnie chronionych – w rozumieniu art. 27 ust. 2 pkt 2 ustawy o ochrony danych osobowych – unormowania, zgodnie z którym administrator danych mógłby upoważnić do przetwarzania danych zawartych w dokumentacji medycznej dowolną, każdą, osobę (art. 24 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 17.02.2015 r.). Zdaniem Generalnego Inspektora Ochrony Danych Osobowych w art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta winny zostać określone kategorie osób niewykonujących zawodów medycznych, które mogą zostać upoważnione przez administratorów danych do przetwarzania danych zawartych w dokumentacji

[171] Dz. U. z 2016 r. poz. 186

medycznej oraz cele dla realizacji których takie upoważnienie do przetwarzania danych może być nadane.

- w związku z zainicjowaniem przez projektodawcę działań legislacyjnych zmierzających do ustalenia zasad dopuszczalności outsourcingu przechowywania dokumentacji medycznej (art. 24 ust. 4–6 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 17.02.2015 r.), organ do spraw ochrony danych osobowych zgłosił do tych regulacji dwie uwagi szczegółowe.

Po pierwsze – przewidziany w art. 24 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 17.02.2015 r., warunek dopuszczalności zawarcia przez podmiot udzielający świadczeń zdrowotnych umowy powierzenia przetwarzania danych zawartych w dokumentacji medycznej, jakim jest zapewnienie przez przetwarzającego ochrony danych osobowych, powinien być rozszerzony o wymóg zagwarantowania przez podmiot, któremu powierzono przetwarzanie danych zawartych w dokumentacji medycznej, zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z wykonywaniem umowy powierzenia (art. 24 ust. 3 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 17.02.2015 r.).

Po drugie – nieprawidłowa jest propozycja z art. 24 ust. 6 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 17.02.2015 r. Mając na uwadze, że przetwarzający działa jedynie na zlecenie podmiotu udzielającego świadczeń zdrowotnych (administratora danych) i na jego rzecz, w przypadku zaprzestania prowadzenia działalności przez podmiot, któremu powierzono przetwarzanie danych zawartych w dokumentacji medycznej, dane te powinny być obligatoryjnie zwracane podmiotowi udzielającemu świadczeń zdrowotnych, który powierzył ich przetwarzanie. Wymaganie takie winno być zamieszczone w przepisach normujących outsourcing przechowywania dokumentacji medycznej.

Uwagi Generalnego Inspektora Ochrony Danych Osobowych skutkowały wprowadzeniem zmian do projektu **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**. Jednocześnie sami autorzy projektu prezentowali rozbieżne koncepcje co do sposobu unormowania niektórych zagadnień.

Dlatego w kolejnej opinii do projektu **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**[172] organ do spraw ochrony osobowych podtrzymał stanowisko w kwestii potrzeby uregulowania mechanizmu wycofywania zgody i sprzeciwu na przetwarzanie danych, tak by prawa usługobiorcy mogły być w pełni realizowane w systemie elektronicznym SIM. Mogłoby to zostać zrealizowane poprzez dodanie w art. 35 ust. 3 b ustawy o systemie informacji w ochronie zdrowia po słowach: „oświadczenia o wyrażeniu zgody albo sprzeciwu" słów: „bądź o wycofaniu zgody albo sprzeciwu".

W przedmiocie normowania zasad dostępu do dokumentacji medycznej innych osób aniżeli wykonujące zawód medyczny – art. 24 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta – Generalny Inspektor Ochrony Danych Osobowych zaproponował uwzględnienie w przepisie możliwości upoważnienia przez administratora danych także innych osób, niż „wykonujące czynności pomocnicze w stosunku do procesu udzielania świadczeń zdrowotnych", gdyż pojęcie to wydawało się nieprecyzyjne i mogło nie obejmować swoim zakresem wszystkich podmiotów, które w związku z funkcjonowaniem systemu ochrony zdrowia mogą przetwarzać dane osobowe usługobiorców. W opinii organu do spraw ochrony danych osobowych należałoby uwzględnić np. osoby odpowiedzialne za utrzymanie systemu teleinformatycznego podmiotu udzielającego świadczeń zdrowotnych oraz za zapewnienie bezpieczeństwa takiego systemu, to jest informatyków, administratora bezpieczeństwa informacji czy administratora systemu informatycznego. Równocześnie Generalny Inspektor Ochrony Danych Osobowych nie zamierzał jednak formułować wyczerpującego katalogu osób, którym dane powinny udostępniane.

Organ do spraw ochrony danych osobowych sugerował też doprecyzowanie art. 24 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta poprzez zmianę końcowej części przepisu. Generalny Inspektor stanął na stanowisku, że podmiot udzielający świadczeń zdrowotnych, który chce skorzystać ze wsparcia podmiotu określonego w art. 31 ust. 1 ustawy o ochronie danych osobowych, powinien mieć taką możliwość, ale pod warunkiem zapewnienia sobie prawa do kontroli zgodności przetwarzania danych przez przetwarzającego (podmiot przyjmujący dane). W obliczu przekazywania innemu podmiotowi do przetwarzania w imieniu i na rzecz administratora danych (podmiotu udzielającego świadczeń zdrowotnych)

[172] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 24 marca 2015 roku do Sekretarza Stanu w Ministerstwie Zdrowia, sygn. DOLiS-033-340/14/TG/24170/15.

danych o stanie zdrowia, czyli danych podlegających szczególnej ochronie[173], konieczne jest zapewnienie w przepisach temu administratorowi jak najbardziej skutecznych możliwości reagowania na ewentualne nieprawidłowości w procesie przetwarzania danych osobowych.

W opinii do projektu **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw** (wersja z dnia 30.03.2015 r.)[174] organ do spraw ochrony danych osobowych poparł podjęcie przez projektodawcę działań zmierzających do unormowania kwestii sposobu postępowania z dokumentacją medyczną po zaprzestaniu udzielania świadczeń zdrowotnych przez podmiot udzielający tych świadczeń. Zwrócił się wszakże o rozważenie, czy w świetle – silnie akcentowanej w orzecznictwie Trybunału Konstytucyjnego – m.in. wyrok Trybunału Konstytucyjnego z dnia 12 lipca 2007 roku[175] – zasady wyłączności ustawy, prawnie dopuszczalne jest zamieszczenie w akcie wykonawczym (rozporządzeniu) przepisów dotyczących tak zasadniczej materii, jaką jest wskazanie podmiotu uprawnionego/zobowiązanego do przejęcia papierowej dokumentacji medycznej „pozostałej" po podmiocie udzielającym świadczeń zdrowotnych, który zaprzestał ich udzielania (art. 30 a ust. 1 pkt 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, dodawany przez art. 10 pkt 4 projektu z 30.03.2015 r.). Propozycja brzmienia komentowanego przepisu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta wzbudziła wątpliwości Generalnego Inspektora Ochrony Danych Osobowych, zwłaszcza w kontekście stanowiska wyrażonego przez Trybunał Konstytucyjny w uzasadnieniu wyroku z dnia 12 lipca 2007 roku[176].

Organ do spraw ochrony danych osobowych ocenił też – zasadniczo – pozytywnie projektowany art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 30.03.2015 r., dotyczący określania zasad dostępu osób do dokumentacji medycznej[177] i outsourcingu danych medycznych[178]. W opinii Generalnego Inspektora Ochrony Danych Osobowych poprawienia wymagał jedynie art. 24 ust. 6 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 1 projektu z 30.03.2015 r., gdyż obowiązek zachowania w tajemnicy informacji

[173] Art. 27 ustawy o ochronie danych osobowych.
[174] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 29 kwietnia 2015 roku do Sekretarza Stanu w Ministerstwie Zdrowia, sygn. DOLiS-033-340/14/TG/34191/15.
[175] Sygn. akt U 7/06
[176] Sygn. akt U 7/06: „Rozporządzenie nie może jednak uzupełniać ustawy, rozbudowywać przesłanek zrealizowania jakiejś normy prawnej, określonej w ustawie, lub takich elementów procedury, które nie odpowiadają jej ustawowym założeniom.".
[177] Art. 24 ust. 2 i 3
[178] Art. 24 ust. 4–7

związanych z pacjentem uzyskanych w związku z realizacją umowy powierzenia przetwarzania danych winien dotyczyć osób, które uzyskają u zleceniobiorcy faktyczny dostęp do danych w następstwie zawarcia tej umowy, nie zaś samego podmiotu, któremu przetwarzanie danych zostało powierzone.

Po wniesieniu do Sejmu Rzeczypospolitej Polskiej projektu **ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw** (druk sejmowy nr 3763), co nastąpiło w dniu 23 lipca 2015 roku, organ do spraw ochrony danych osobowych w dalszym ciągu uczestniczył w pracach legislacyjnych. Ze względu na specyfikę tych prac, przejawiającą się w usuwaniu z projektu z druku nr 3763 niektórych już przyjętych rozwiązań i wprowadzaniu nowych unormowań, których konieczność uchwalenia ujawniła się na etapie sejmowym prac legislacyjnych, zaszła potrzeba zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych poprawek do projektu z druku nr 3763 dotyczących outsourcingu danych medycznych.

Uwzględniając szczególny charakter – mających być powierzanymi – danych dotyczących najintymniejszych sfer życia człowieka, organ do spraw ochrony danych osobowych wniósł[179] o uzupełnienie (proponowanego) art. 9 a ustawy o systemie informacji w ochronie zdrowia o ustęp: „Podmioty, o których mowa w ust. 2, są zobowiązane do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją umowy, o której mowa w ust. 1. Podmioty te są związane tajemnicą także po śmierci pacjenta".

Analogicznie – w projektowanym art. 20 ustawy o systemie informacji w ochronie zdrowia Generalny Inspektor Ochrony Danych Osobowych proponował ustęp: „Podmioty, o których mowa w ust. 6, są zobowiązane do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją umowy, o której mowa w ust. 5. Podmioty te są związane tajemnicą także po śmierci pacjenta".

W opinii organu do spraw ochrony danych osobowych, w świetle dyspozycji art. 31 ust. 1 ustawy o ochronie danych osobowych, celowym byłoby również poprawienie brzmienia (proponowanych) art. 9 a ust. 4 i art. 20 ust. 8 ustawy o systemie informacji w ochronie zdrowia. Artykuł 9 ustęp 4: „Podmioty, o których mowa w ust. 2, nie mogą powierzać innym podmiotom przetwarzania danych, o których mowa w ust. 1" oraz artykuł 20 ustęp 8:

[179] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 3 września 2015 roku do Naczelnik Wydziału Prawnego w Departamencie Infrastruktury i e-Zdrowia w Ministerstwie Zdrowia, sygn. DOLiS-033-340/14/TG/80929/15.

„Podmioty wyspecjalizowane w zapewnianiu obsługi technicznej systemów teleinformatycznych, o których mowa w ust. 5, nie mogą powierzać innym podmiotom przetwarzania danych zawartych w rejestrach medycznych".

Stwierdzić należy, iż uchwalona przez Parlament RP i podpisana przez Prezydenta RP **ustawa z dnia 9 października 2015 roku o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw** uwzględnia w swojej treści szereg uwag i zastrzeżeń Generalnego Inspektora Ochrony Danych Osobowych, tym samym stanowi istotny krok naprzód w kwestii zapewnienia właściwego poziomu ochrony danych medycznych i praw pacjentów. Organ do spraw ochrony danych osobowych akceptuje przyjęte w niej unormowania za wyjątkiem jej art. 10 pkt 5, wprowadzającego nowe brzmienie art. 30 a ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta regulującego sposób postępowania z dokumentacją medyczną po zaprzestaniu udzielania świadczeń zdrowotnych przez podmiot udzielający świadczeń zdrowotnych. Generalny Inspektor Ochrony Danych Osobowych stoi na stanowisku, iż znowelizowany art. 30 a ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta prawidłowo normuje jedynie sposób postępowania z elektroniczną dokumentacją medyczną wytworzoną przez podmiot udzielający świadczeń zdrowotnych, który zaprzestał udzielania świadczeń zdrowotnych[180], zaś jest niewystarczający w odniesieniu do papierowej dokumentacji medycznej[181]. Co więcej – art. 30 a ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta pomija milczeniem kwestię sposobu postępowania z wytworzoną dokumentacją medyczną w razie śmierci lekarza albo pielęgniarki wykonujących zawód w ramach indywidualnej praktyki bądź ich całkowitej rezygnacji z zawodu.

Pozytywny efekt w postaci poprawienia, pierwotnie kontrowersyjnych, rozwiązań prawnych przyniosły także uwagi Generalnego Inspektora Ochrony Danych Osobowych do projektu **ustawy o zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw**[182].

W opinii do tego projektu[183] organ do spraw ochrony danych osobowych zakwestionował – zawartą w art. 1 pkt 4 projektu – propozycję nowego przepisu ustawy z dnia 12 października 1990 roku o Straży Granicznej[184] – art. 10aa.

[180] Art. 30 a ust. 1 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 5 ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw.
[181] Art. 30 a ust. 1 pkt 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w brzmieniu nadanym przez art. 10 pkt 5 ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw.
[182] DOLiS-033-92/15
[183]Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 23 marca 2015 roku do Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych, DOLiS-033-340/14/KK/23359.
[184] Dz. U. z 2014 r. poz. 1402 z późn. zm.

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych brak było bowiem uzasadnienia dla przyznania Straży Granicznej prawa dostępu do policyjnych baz danych w trybie bezwnioskowym (automatycznym) za pomocą systemu teleinformatycznego. Zaproponowany w kwestionowanym przepisie tryb udostępniania danych pozbawiał administratora danych (Policję) możliwości weryfikacji zasadności i celowości pozyskania z jej zbiorów danych (w tym Krajowego Systemu Informacyjnego Policji) informacji, w tym danych osobowych, o osobach poszukiwanych. Równocześnie zaś – wskazany w art. 10 aa ust. 1 ustawy o Straży Granicznej, dodawanym przez art. 1 pkt 4 projektu, cel przedmiotowej regulacji, którym miało być wykonywanie przez Straż Graniczną czynności zleconych przez właściwe organy państwowe, nie przemawiał – w ocenie organu do spraw ochrony danych osobowych – za wprowadzeniem rozwiązania tak dalece ingerującego w uprawnienia Policji jako administratora danych, zwłaszcza że w ustawie o Straży Granicznej znajdują się już unormowania umożliwiające tej służbie pozyskiwanie danych od innych organów państwowych.

Generalny Inspektor Ochrony Danych Osobowych stanął także na stanowisku, iż – zamieszczona w art. 2 projektu – propozycja brzmienia nowego przepisu ustawy z dnia 21 marca 1985 roku o drogach publicznych[185] – art. 20 g – jest niewystarczająca.

Z przepisu w kształcie zaproponowanym w projekcie nie wynikało w sposób jednoznaczny: 1) czy montowane w pasie drogowym dróg na obszarze strefy nadgranicznej stacjonarne urządzenia będą rejestrować jedynie obraz, czy też obraz i dźwięk, 2) czy dane zgromadzone w procesie monitorowania będą przechowywane w samych urządzeniach monitorujących, czy też przesyłane za pomocą sieci telekomunikacyjnych, 3) czy podmioty, którym Straż Graniczna będzie zlecać montaż, demontaż i obsługę techniczną przedmiotowych urządzeń uzyskają (choćby potencjalną) możliwość dostępu do danych zgromadzonych w ramach monitoringu.

Projektodawca udzielił obszernej odpowiedzi[186], w której rozstrzygnął wątpliwości Generalnego Inspektor Ochrony Danych Osobowych w odniesieniu do (projektowanego) art. 20 g ustawy o drogach publicznych i przedstawił kompromisową propozycję dyspozycji (proponowanego) art. 10aa ustawy o Straży Granicznej. Zgodnie z nią Straż Graniczna miałaby jedynie dostęp do wyodrębnionej repliki policyjnej bazy danych zawierającej tylko

[185] Dz. U. z 2015 r. poz. 460 z późn. zm.

[186] Pismo Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych z dnia 2 kwietnia 2015 roku – znak: DP-I-0231-91/2014/ES.

informacje o osobach poszukiwanych, o których mowa w art. 20 ust. 2 a pkt 5 ustawy z dnia 6 kwietnia 1990 roku o Policji[187].

Biorąc pod uwagę, iż – wyżej zaprezentowana – propozycja Ministerstwa Spraw Wewnętrznych została jeszcze w projekcie **ustawy o zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw** (wersja z dnia 15.04.2015 r.) uzupełniona o obowiązek Straży Granicznej informowania Policji (administratora danych) o odnalezieniu osoby poszukiwanej (co służyć będzie wzmocnieniu procesu weryfikacji przez Policję zasadności i celowości pozyskiwania przez Straż Graniczną danych z jej zbioru danych), jak również uwzględniając cel projektowanej regulacji, którym jest zapewnienie Straży Granicznej możliwości skutecznego wykonywania jej zadań, w tym niedopuszczenie do przekraczania granic Rzeczypospolitej Polskiej przez osoby poszukiwane, organ do spraw ochrony danych osobowych uznał brzmienie art. 10 aa ustawy o Straży Granicznej z projektu **ustawy o zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw** (wersja z dnia 15.04.2015 r.) za akceptowalne[188].

Projekt **ustawy o zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw** został uchwalony przez Parlament i podpisany przez Prezydenta Rzeczypospolitej Polskiej jako **ustawa z dnia 9 lipca 2015 roku o zmianie ustawy o Straży Granicznej oraz niektórych innych ustaw**[189].

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

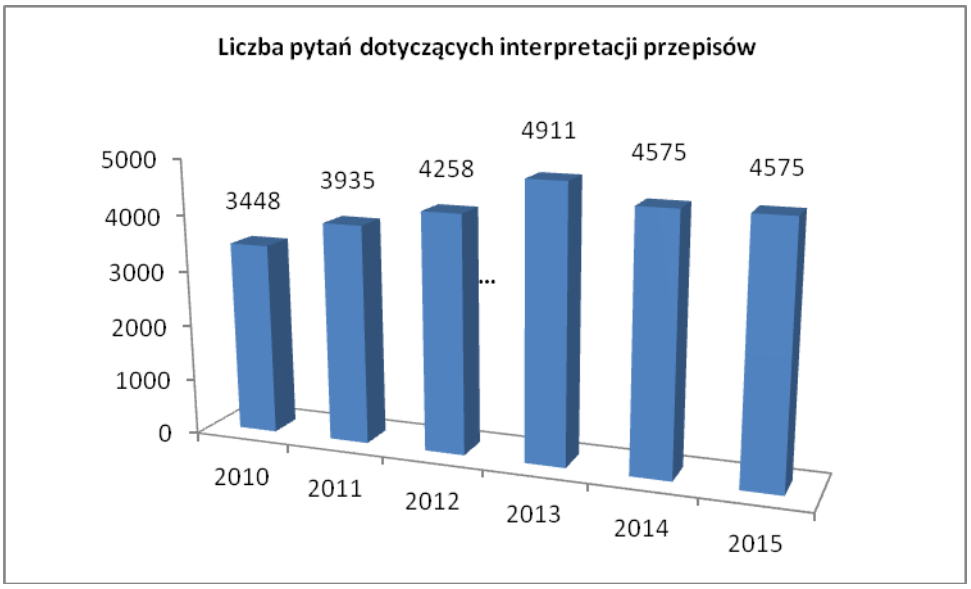
Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych, stanowi bardzo ważną część działalności Generalnego Inspektora Ochrony Danych Osobowych. Działania te obejmują szeroko zakrojone działania informacyjne i edukacyjne, których różnorodna forma i dynamika ma wpływ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

[187] Dz. U. z 2015 r. poz. 355 z późn. zm.
[188] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 21 kwietnia 2015 roku do Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych, sygn. DOLiS-033-92/15/TG/31751.
[189] Dz. U. z 2015 r. poz. 1336

9.1. 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 2015 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło **3962 pytania prawnych** z prośbą o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, bądź sygnalizujących różnego rodzaju problemy interpretacyjne związane z ich przestrzeganiem.



Wykres 34: ***Zestawienie porównawcze liczby pytań dotyczących interpretacji przepisów z zakresu ochrony danych osobowych skierowanych do GIODO w latach - 2010–2015.***

Wartym zauważenia jest, iż liczba zapytań dotyczących interpretacji przepisów prawa w 2015 r. w porównaniu do roku 2014 zmniejszyła się o prawie 14 %. 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 oczekiwane

rezultaty, co jednak nie oznacza, że zainteresowanie pozyskiwaniem informacji w formie odpowiedzi na pytania znacząco spadło.

Podobnie jak w latach poprzednich, także w roku 2015, 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, danych osobowych. Pojawiały się ponadto pytania o dopuszczalność przekazywania danych osobowych innym instytucjom publicznym oraz osobom prywatnym – np. w celach naukowych. 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. Niezmiennie ważne były również kwestie dostępu do systemów teleinformatycznych wspomagających realizację zadań do ww. sektorach i funkcjonalności tychże systemów umożliwiających dostęp lub przetwarzanie dodatkowych danych, zbędnych z punktu widzenia realizacji pewnych celów.
2) **Szkolnictwa** – np. dotyczące monitorowania losów absolwentów czy dostępu do dokumentacji przez organ sprawujący nadzór nad szkołą. Wątpliwości dotyczyły również wprowadzenia numeru PESEL ucznia na legitymacji szkolnej.
3) **Instytucji finansowych** – kwestia wymiany przez kredytodawców informacji dotyczących konsumentów, w celu dokonywania oceny zdolności kredytowej, pytania dotyczące przetwarzania przez BIK danych osobowych pochodzących z publicznie dostępnych jawnych rejestrów, m.in. z rejestru KRS, REGON, CEIDG, a także przetwarzania danych biometrycznych klientów przez banki. Liczne pytania dotyczyły zagadnień związanych z tzw. tajemnicą bankową.
4) **Służby Zdrowia** – w odniesieniu do podstaw przetwarzania danych o stanie zdrowia, w tym udostępnienia takich danych przez podmioty lecznicze innym podmiotom, np. Policji czy Zakładowi Ubezpieczeń Społecznych.
5) **Zatrudnienia –** pojawiały się pytania dotyczące dopuszczalnego zakresu danych pozyskiwanych zarówno od kandydatów do pracy, jak i pracowników, a także

przesłanek legalizujących wykorzystywanie danych przez pracodawców, w tym przekazywania danych osobowych pracowników podmiotom zewnętrznym. Wiele pytań dotyczyło różnych form kontroli pracownika przez pracodawcę oraz granic ich dopuszczalności (w tym wykorzystywania danych biometrycznych do kontroli czasu pracy), czy też wglądu do akt pracowniczych w przypadku kontroli przeprowadzanej u pracodawcy. Pytania odnosiły się ponadto do udostępniania przez pracodawcę list z wyszczególnionymi powodami nieobecności pracowników oraz działalności społecznych inspektorów pracy i związków zawodowych. Do Generalnego Inspektora Ochrony Danych Osobowych docierały ponadto sygnały na temat fałszywych ofert pracy wykorzystywanych do pozyskiwania danych osobowych i skanów lub kserokopii dowodów osobistych.

6) **Mieszkalnictwa –** zapytania zarówno od zarządów, jak i członków wspólnot oraz spółdzielni mieszkaniowych, dotyczące przetwarzania danych osobowych w związku z zarządzaniem nieruchomościami, w tym także lokalami komunalnymi.
7) **Telekomunikacji i Internetu** - pytania dotyczące tego, czy tzw. nick (internetowy pseudonim użytkownika) albo numer IP komputera, należy traktować jako daną osobową; liczna tez była korespondencja dotycząca przesyłania spamu. Pojawiały się również pytania związane z zakresem danych osobowych wymaganych przy korzystaniu z różnych usług świadczonych drogą elektroniczną oraz konieczności wyrażenia zgody na przesyłanie korespondencji o charakterze marketingowym, jako warunku skorzystania z określonej usługi online.
8) **Monitoringu**, w tym wykorzystania urządzeń rejestrujących zarówno przez osoby fizyczne, jak i monitoringu wizyjnego stosowanego przez różnego rodzaju podmioty, wykorzystywania monitoringu wizyjnego w szpitalach i zakładach pracy, udostępniania nagrań z wideo monitoringu, jak również rejestracji dźwięku włącznie z rejestracją obrazu.
9) **Innych** zagadnień dotyczących ochrony danych osobowych – w tym żądania kserokopii i skanów dowodu tożsamości przez różne podmioty oraz oddawania tych dokumentów „w zastaw" jako warunku skorzystania z określonej usługi. Wzrasta również liczna zapytań o podstawę prawną udzielania informacji w przypadku egzekucji komorniczych.

Powyżej przytoczone przykłady pozostają oczywiście jedynie częścią tematyki wpływających do Biura GIODO zagadnień obejmującej wszakże wszystkie właściwie dziedziny życia publicznego.

9.2. Wystąpienia

Mocą art. 19a ustawy o ochronie danych osobowych, w celu realizacji zadań, o których mowa w art. 12 pkt 6, Generalny Inspektor Ochrony Danych Osobowych może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów, **wystąpienia** zmierzające do zapewnienia skutecznej ochrony danych osobowych (ust 1). Generalny Inspektor może również występować do właściwych organów - z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych (ust. 2). Podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania (ust 3).

W 2015 roku Generalny Inspektor Ochrony Danych Osobowych skierował **80 takich wystąpień,** z czego **57 wystąpień w trybie art. 19a ustawy o ochronie danych osobowych.** Poniżej przedstawione zostały przykłady 17 wystąpień Generalnego Inspektora skierowanych **do podmiotów administracji publicznej** w celu dostosowania obecnie obowiązujących przepisów prawa do zasad prawidłowego przetwarzania danych osobowych.

Poniżej przedstawione zostały przykłady najważniejszych przedmiotowych wystąpień GIODO:

1) wystąpienie w związku z pozyskiwaniem szerokiego zakresu danych osobowych od osób odwiedzających miejskie muzeum

Generalny Inspektor Ochrony Danych Osobowych pozyskał informację na temat ankiety, która – na polecenie władz miasta– miała być kierowana do osób odwiedzających muzeum. Za pośrednictwem ankiety miały być zbierane dane osobowe zwiedzających, takie jak imię i nazwisko, adres e-mail, miejscowość i rok urodzenia. Informacje te miały być uzupełniane o odpowiedzi na pytania dotyczące zwiedzania muzeum oraz pobytu w mieście (długość, cel i miejsce pobytu).

W piśmie z dnia 17 kwietnia 2015 r.[190]skierowanym do burmistrza miasta Generalny Inspektor wskazał, iż w ten sposób powstać może zbiór danych osobowych zawierający szeroki zakres informacji, w tym związanych z preferencjami osób, które wypełniają ankietę. Powołując się na art. 51 ust. 2 Konstytucji RP[191] oraz art. 23 ust. 1 ustawy o ochronie danych osobowych[192], organ podkreślił, iż władze miasta, pozyskując dane od osób zwiedzających muzeum, powinny dysponować przesłanką legalizującą przetwarzanie tych danych – w postaci przepisu prawa lub zgody osoby, której dane dotyczą. Jeśli zaś przetwarzanie danych osobowych miałoby się odbywać się podstawie zgody osoby, której dane dotyczą, zgoda ta powinna spełniać kryteria określone w art. 7 pkt 5 ustawy o ochronie danych osobowych[193].

Generalny Inspektor jednocześnie przypomniał, że administrator danych ma obowiązek, zgodnie z art. 24 ust. 1 pkt 4 ustawy o ochronie danych osobowych, poinformować osobę, której dane dotyczą o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej. Konieczne jest również poinformowanie osoby, której dane dotyczą o celu zbierania danych, a w szczególności o znanych administratorowi w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych (art. 24 ust. 1 pkt 2 ustawy). Przetwarzanie danych osobowych powinno również w każdym przypadku następować zgodnie z zasadami legalizmu, adekwatności, celowości i ograniczenia czasowego, określonymi w przepisach ustawy o ochronie danych osobowych[194].

---

[190] DOLiS-035-451/15

[191] Art. 51 ust. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

[192] Art. 23.1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: 1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych; 2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; 3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; 4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; 5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. 2. Zgoda, o której mowa w ust. 1 pkt 1, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania. 3. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w ust. 1 pkt 1 jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe. 4. 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.

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

[194] Art. 26. 1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: 1) przetwarzane zgodnie z prawem; 2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2; 3) merytorycznie poprawne i

W opinii Generalnego Inspektora zachodziła wątpliwość, czy w analizowanym przypadku rzeczywiście istniał cel, który uzasadniałby w sposób wystarczający zbieranie danych pozwalających na zidentyfikowanie konkretnych osób. Innymi słowy, czy odpowiedzi na pytania dotyczące muzeum oraz miasta zamieszczone w ankiecie wymagały posiadania przez władze miasta również danych identyfikujących poszczególne osoby odwiedzające muzeum. Wydaje się, iż cel, jakiemu ma służyć ankieta mógłby zostać spełniony również bez konieczności podawania przez osoby ją wypełniające imion, nazwisk, adresów e-mail, miejscowości i roku urodzenia – ankieta mogłaby mieć wobec tego charakter anonimowy.

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych zwrócił się do burmistrza miasta o podjęcie działań mających na celu zaprzestanie nie znajdującego uzasadnienia i podstawy prawnej pozyskiwania danych osobowych oraz podjęcie działań mających na celu wyeliminowanie podobnych nieprawidłowości w przyszłości.

W piśmie z dnia 11 maja 2015 r. urząd miejski przekazał Generalnemu Inspektorowi stanowisko dyrektora muzeum, zawierające poprawiony, zgodnie z sugestiami organu, blankiet ankiety.

2) wystąpienie dotyczące pozyskiwania szerokiego zakresu danych osobowych od mieszkańców gminy wypełniających na stronie urzędu gminy ankietę dotyczącą planu gospodarki niskoemisyjnej

W związku z pozyskaniem przez Generalnego Inspektora Ochrony Danych Osobowych informacji o tym, że na stronie internetowej Biuletynu Informacji Publicznej urzędu gminy została zamieszczona ankieta dotycząca planu gospodarki niskoemisyjnej, za pośrednictwem której zbierany jest szeroki zakres informacji na temat mieszkańców gminy – organ do spraw ochrony danych osobowych skierował w dniu 17 kwietnia 2015 r. do wójta gminy wystąpienie[195], w którym zwrócił się o zmianę opisanej praktyki.

W wystąpieniu Generalny Inspektor podkreślił, iż z uwagi na treść art. 51 ust 2 Konstytucji RP oraz art. 23 ust. 1 ustawy o ochronie danych osobowych, urząd gminy, pozyskując dane od mieszkańców na potrzeby opracowania planu gospodarki niskoemisyjnej w gminie, powinien dysponować przesłanką legalizującą przetwarzanie tych danych – w postaci przepisu prawa lub zgody osoby, której dane dotyczą. Jednocześnie, administrator

adekwatne w stosunku do celów, w jakich są przetwarzane; 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. 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.

[195] DOLiS-035-750/15

danych ma obowiązek, zgodnie z art. 24 ust. 1 pkt 4ustawy o ochronie danych osobowych, poinformować osobę, której dane dotyczą o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Zachodziła wątpliwość, czy w analizowanym przypadku rzeczywiście istniał cel, który uzasadniałby w sposób wystarczający zbieranie danych pozwalających na zidentyfikowanie konkretnych osób. Innymi słowy, czy dla opracowania planu gospodarki niskoemisyjnej wymagane jest posiadanie przez gminę zindywidualizowanych danych osobowych mieszkańców. Wydaje się, iż cel, jakiemu ma służyć ankieta mógłby zostać spełniony również bez konieczności podawania przez osoby ją wypełniające imion, nazwisk, adresów i numerów telefonów – ankieta mogłaby mieć wobec tego charakter anonimowy. W połączeniu z pozostałymi informacjami, jakie mają być udostępniane przez mieszkańców gminy, dochodziłoby w rezultacie do pozyskiwania bardzo szerokiego zakresu danych na temat osób wypełniających ankietę, co wydaje się zbędne, a zatem nieadekwatne w stosunku do zamierzonego celu.

Powyższe należy oceniać z punktu widzenia zasady adekwatności, która oznacza, że dane osobowe nie mogą być zbierane na zapas, „na wszelki wypadek", tj. bez wykazania celowości ich pozyskania i niezbędności dla realizacji zadań administratora danych. Administrator danych, dla uznania legalności swojego działania, musi – poza wykazaniem istnienia podstawy prawnej upoważniającej do przetwarzania danych osobowych – uczynić zadość zasadzie adekwatności. Adekwatność danych w stosunku do celu ich przetwarzania powinna być natomiast rozumiana jako równowaga pomiędzy dobrem osoby, której dane dotyczą, a interesem administratora danych. Oznacza to, że administrator danych nie może przetwarzać danych w zakresie szerszym, niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem, stopniu szczegółowości.

W tym stanie rzeczy zachodziła potrzeba dokonania rzetelnej analizy, celem ograniczenia zakresu danych udostępnianych za pośrednictwem ankiety do informacji rzeczywiście niezbędnych ze względu na cel, jakim jest opracowanie planu gospodarki niskoemisyjnej w gminie – o co Generalny Inspektor Ochrony Danych Osobowych zwrócił się do wójta.

Dnia 11 maja 2015 r. urząd gminy skierował do Generalnego Inspektora pismo, w którym poinformowano, iż gmina zastosowała się do uwag organu.

3) wystąpienie w związku z nieprawidłowym przechowywaniem korespondencji skierowanej do petentów urzędu miejskiego

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych skierował również wystąpienie[196] do prezydenta miasta (dnia 13 kwietnia 2015 r.) – w związku z pozyskaniem informacji o tym, że niedoręczona w danym dniu korespondencja adresowana do petentów urzędu miejskiego jest przechowywana w domach prywatnych pracowników urzędu zajmujących się doręczaniem przesyłek. Rozwiązanie to miało wynikać z faktu, iż korespondencja jest doręczana do godziny 21:30 (podczas gdy urząd pracuje do godziny 15:30), zatem niedoręczone listy nie mogą być danego dnia przekazane z powrotem do urzędu. Opisana praktyka wzbudziła poważne wątpliwości organu pod względem jej zgodności z przepisami ustawy o ochronie danych osobowych.

Generalny Inspektor wskazał, iż jednym z podstawowych obowiązków spoczywających na administratorze jest, wynikający z art. 36 ust. 1 ustawy o ochronie danych osobowych, 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.

Z art. 36 ust. 2 wynika natomiast obowiązek prowadzenia przez administratora dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Dokumentacja taka powinna określać m.in. wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe. Zgodnie zaś z art. 37 ustawy o ochronie danych osobowych, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Osoby, które zostały upoważnione do przetwarzania danych, są zaś obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 ust. 2 ustawy).

Wszelkie czynności związane z przetwarzaniem danych osobowych winny być wykonywane z uwzględnieniem wszelkich środków technicznych i organizacyjnych zapewniających ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym. Z powyższego wynika zatem, że ich odpowiedniego zastosowania wymaga nie tylko proces przetwarzania danych osobowych w systemach informatycznych, czy w zbiorach tradycyjnych,

[196] DOLiS-035-756/15

ale także każda inna wykonywana na nich operacja, zatem i proces przechowywania dokumentów zawierających dane osobowe.

W swoim wystąpieniu Generalny Inspektor podkreślił ponadto, że administrator danych może ponosić odpowiedzialność karną na gruncie przepisów art. 51 ust. 1 oraz art. 52 ustawy o ochronie danych osobowych[197] oraz że stosowana przez Urząd Miejski praktyka, stanowiąca przyczynek do wystąpienia stwarza zagrożenie dla tajemnicy korespondencji, podlegającej ochronie na gruncie art. 49 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

Organ zwrócił także uwagę na art. 41 ust. 3 ustawy z dnia 23 listopada 2012 r. Prawo pocztowe (Dz. U. z 2012 r. poz. 1529 z późn. zm.), określający na czym polega naruszenie obowiązku zachowania tajemnicy pocztowej[198] oraz na art. 267 §1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z poźn. zm.), zgodnie z którym kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo (…) podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

W związku z przedstawionymi powyżej zastrzeżeniami, Generalny Inspektor zwrócił się do prezydenta miasta o podjęcie działań mających na celu zaprzestanie praktyki przechowywania korespondencji kierowanej do petentów Urzędu Miejskiego w prywatnych domach pracowników urzędu zajmujących się doręczaniem przesyłek oraz podjęcie działań mających na celu wyeliminowanie podobnych nieprawidłowości w przyszłości.

W odpowiedzi na wystąpienie, prezydent miasta poinformował, iż cała korespondencja niedoręczona w danym dniu jest po zakończeniu pracy deponowana w siedzibie Straży Miejskiej w zamykanych boksach odrębnie dla każdego gońca. Zasady te wprowadzono od dnia 8 maja 2015 r.

[197] 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.

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.

[198] Art. 41 ust. 3. Naruszeniem obowiązku zachowania tajemnicy pocztowej jest w szczególności: 1) ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową; 2) otwieranie zamkniętych przesyłek pocztowych lub zapoznawanie się z ich treścią; 3) umożliwianie osobom nieuprawnionym podejmowania działań mających na celu wykonywanie czynności, o których mowa w pkt 1 i 2.

4) wystąpienie z związku z udostępnieniem danych osobowych osoby fizycznej (w tym również danych szczególnie chronionych) w odpowiedzi na wniosek o udostępnienie informacji publicznej

Generalny Inspektor Ochrony Danych Osobowych pozyskał informację o udostępnieniu danych osobowych osoby fizycznej (osoby prowadzącej szkołę nauki jazdy), w tym tzw. danych szczególnie chronionych, w odpowiedzi na wniosek o udostępnienie informacji publicznej na temat sposobu nadzorowania nad ośrodkami szkolenia kierowców, w związku z czym skierował do prezydenta miasta wystąpienie[199] (dnia 9 lutego 2015 r.), w którym zwrócił się o wyeliminowanie takich działań.

W pierwszej kolejności Generalny Inspektor wskazał na przepisy Konstytucji RP stanowiące źródło ochrony prywatności osoby, której dane dotyczą oraz art. 23 ust. 1 i art. 27 ust. 2 ustawy o ochronie danych osobowych[200], które określają przesłanki legalności przetwarzania, w tym udostępniania danych osobowych.

Organ przypomniał następnie, iż zgodnie z art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2015 r. poz. 2058, z późn. zm.), prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub

[199] DOLiS-035-751/14

[200] 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 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.

tajemnicę 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. Prywatność określonej osoby jako dobro chronione prawem, powinno mieć pierwszeństwo przed innym dobrem prawem chronionym – dostępem do informacji publicznej.

Trybunał Konstytucyjny wielokrotnie w wydanych orzeczeniach wyrażał pogląd, iż prawo dostępu do informacji nie ma charakteru bezwzględnego, a jego granice wyznaczone są m.in. przez konieczność respektowania praw i wolności innych podmiotów, w tym przez konstytucyjnie gwarantowane prawo do ochrony życia prywatnego (wyrok z dnia 20 marca 2006 r., sygn. akt K 17/2005). Trybunał stwierdził również, że w ramach zderzenia się dwóch wartości – z jednej strony konstytucyjnego prawa do informacji, z drugiej prawa do prywatności – nie można bezwzględnie przyznać priorytetu temu pierwszemu.

Generalny Inspektor podkreślił, że dla udostępnienia danych osobowych niezbędne jest istnienie ku temu odpowiedniej podstawy prawnej (art. 26 ust 1 pkt 1, art. 23 ust. 1, art. 27 ustawy o ochronie danych osobowych), zaś przepisy ustawy o dostępie do informacji publicznej są podstawą do udostępnienia jedynie informacji publicznej. Z punktu widzenia niniejszej sprawy istotny był również obowiązek ustanowiony w art. 26 ust. 1 pkt 3 ustawy, zgodnie z którym administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Udostępnienie dokumentu, który zawiera dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, może nastąpić po odpowiednim przetworzeniu (zanonimizowaniu) danych osobowych w nim zawartych. Udostępniając informację publiczną w sposób ingerujący w prywatność osoby fizycznej administrator danych obowiązany jest zatem ustalić czy zakres przekazywanych danych jest niezbędny dla potrzeb takiego udostępnienia.

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych zwrócił się do prezydenta miasta o zaprzestanie nie znajdującego podstawy prawnej udostępniania danych osobowych osób fizycznych.

W odpowiedzi na wystąpienie (z dnia 12 marca 2015 r.) wyjaśniono, iż opisany przez Generalnego Inspektora fakt w zakresie danych osobowych zwykłych miał miejsce zgodnie z

obowiązującymi przepisami prawa, natomiast w zakresie danych osobowych szczególnie chronionych nie miał miejsca.

5) wystąpienie z wnioskiem o wprowadzenie zmian w ustawie Prawo zamówień publicznych w zakresie regulacji dotyczących przetwarzania danych osobowych

Dnia 26 marca 2015 r. Generalny Inspektor skierował wystąpienie[201] do Prezesa Rady Ministrów, z wnioskiem o rozważenie wprowadzenia w przepisach ustawy Prawo zamówień publicznych zmian w zakresie regulacji dotyczących przetwarzania danych osobowych.

W związku z sygnalizowanymi Generalnemu Inspektorowi Ochrony Danych Osobowych wątpliwościami i zastrzeżeniami dotyczącymi stosowania przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. 2015 r. poz. 2164), w zakresie publikowania na stronach internetowych instytucji publicznych i w Biuletynie Informacji Publicznej danych osobowych w zakresie imion i nazwisk oraz pełnych adresów zamieszkania osób fizycznych, organ wskazał, iż obecne regulacje zawarte w ustawie Prawo zamówień publicznych prowadzą do nadmiernej ingerencji w prywatność osób, których te dane dotyczą, oraz osób trzecich pozostających w określonych relacjach z podmiotami danych[202]. Jako przykład Generalny Inspektor przywołał skargi dotyczące udostępnienia na stronie internetowej warszawskiego Zarządu Transportu Miejskiego szerokiego zakresu danych osób, które wzięły udział w przetargu ograniczonym na usługi kontroli biletów oraz uprawnień pasażerów korzystających z usług lokalnego transportu zbiorowego w Warszawie.

Budzące wątpliwość Generalnego Inspektora regulacje dotyczyły publikowania danych osobowych, w tym również adresów zamieszkania wykonawców oraz autorów prac konkursowych (a zatem również osób fizycznych). Ponadto, część z tych kwestionowanych przepisów posługiwała się sformułowaniem „co najmniej", przez co katalog udostępnianych danych zyskuje charakter otwarty – rozwiązanie takie może w konsekwencji prowadzić do nieuzasadnionego udostępniania zbyt szerokiego zakresu danych.

W związku z powyższym, organ zwrócił się o zainicjowanie prac legislacyjnych celem usunięcia z przepisów ustawy Prawo zamówień publicznych postanowień w zakresie obowiązku udostępniania danych osobowych – w postaci adresu zamieszkania osób biorących udział w postępowaniach wskazanych w przedmiotowej ustawie – nieoznaczonemu kręgowi odbiorców za pośrednictwem m.in. sieci Internet oraz celem ograniczenia katalogu tych

[201] DOLiS-035-1082/15

[202] Kwestionowane przez GIODO regulacje znajdowały się art. 62 ust. 2a pkt 4, art. 66 ust. 2 pkt 4, art. 80 ust. 2, art. 86 ust. 4, art. 92 ust. 1 pkt 1 oraz ust. 2, art. 123 ust. 1 ustawy Prawo zamówień publicznych.

danych poprzez wyeliminowanie sformułowań pozwalających na jego poszerzanie. Nie umniejszając konieczności zapewnienia przejrzystości przeprowadzania postępowań z zakresu zamówień publicznych, wskazać należy, iż zmiana przepisów zapewniłaby spójność całego systemu prawa w zakresie zarówno realizacji idei transparentności organów władzy publicznej, jak i prawa obywateli do prywatności. Realizacja zamówień publicznych przeprowadzana być powinna oczywiście w sposób zapewniający całkowitą transparentność, niemniej jednak nie można uznać, iż przepisy ustawy o zamówieniach publicznych są wystarczającym gwarantem ochrony prywatności.

Generalny Inspektor podkreślił, iż zapewnienie jawności i przejrzystości życia publicznego nie może odbywać się kosztem przestrzegania zasad ochrony prywatności i danych osobowych oraz, że „należy rozważyć, czy zastosowane w przepisach ustawy środki są niezbędne do osiągnięcia zamierzonego celu oraz czy celu tego nie da się osiągnąć w inny sposób, tj. poprzez upublicznienie węższego zakresu informacji o osobach. Jako przykład uregulowań dotyczących podobnych zagadnień, a jednocześnie uwzględniających ochronę prywatności osób fizycznych wskazać można regulacje dotyczące oświadczeń majątkowych – w których mimo ich upublicznienia nie dochodzi do zamieszczania adresów zamieszkania osób, których przedmiotowe oświadczenia dotyczą". W opinii Generalnego Inspektora zakres danych, jakie są udostępniane na mocy kwestionowanych przepisów ustawy Prawo zamówień publicznych, jest nadmierny, zwłaszcza biorąc pod uwagę publikację tych danych w Internecie i wiążące się z tym ryzyka.

Wystąpienie GIODO zostało przekazane Urzędowi Zamówień Publicznych, który nie podzielił wątpliwości organu, stwierdzając, iż publikacja danych osobowych wynika z unijnych dyrektyw, których ustawa Prawo zamówień publicznych stanowi implementację.

6) wystąpienie do Ministra Środowiska dotyczące treści deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi

W związku z sygnalizowanymi Generalnemu Inspektorowi Ochrony Danych Osobowych wątpliwościami i zastrzeżeniami dotyczącymi stosowania przepisów ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (Dz. U. z 2016 r. poz. 250) w zakresie, w jakim regulują one kwestie związane z koniecznością udostępniania danych osobowych w treści deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, organ skierował wystąpienie do Ministra Środowiska[203]. Generalny Inspektor

[203] DOLiS-035-710/15

przypomniał jednocześnie, iż przepisy ustawy były również przedmiotem wystąpienia, jakie 27 maja 2013 r. skierował do Ministra Administracji i Cyfryzacji[204], wskazując na konieczność respektowania przepisów o ochronie danych osobowych w treści uchwał organów jednostek samorządu terytorialnego, określających m.in. wzory deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi.

Zgodnie z art. 6m ustawy o utrzymaniu czystości i porządku w gminach, właściciel nieruchomości jest obowiązany złożyć do wójta, burmistrza lub prezydenta miasta deklarację o wysokości opłaty za gospodarowanie odpadami komunalnymi w terminie 14 dni od dnia zamieszkania na danej nieruchomości pierwszego mieszkańca lub powstania na danej nieruchomości odpadów komunalnych (ust. 1). Deklaracja zawiera dane niezbędne do określenia wysokości opłaty za gospodarowanie odpadami komunalnymi oraz wysokość opłaty za gospodarowanie odpadami komunalnymi (ust. 1a). W art. 6m ust. 1b wskazano katalog danych, których może wymagać rada gminy określając wzór deklaracji[205]. W opinii Generalnego Inspektora, wskazany w przepisach zakres danych jest zbyt szeroki do realizacji celów wynikających z ustawy o utrzymaniu czystości i porządku w gminach.

Generalny Inspektor wskazał, iż jakkolwiek uchwała może uprawniać organy gminy do żądania od właścicieli nieruchomości tzw. danych zwykłych (imię, nazwisko, adres zamieszkania) to nie może jednocześnie zezwalać na pozyskiwanie danych w nadmiarze, danych nieadekwatnych w stosunku do celu ich przetwarzania, a co za tym idzie – oczywiście zbędnych. Organy gminy, jako administratorzy danych w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych[206], dla uznania legalności ich działania muszą bowiem, poza wykazaniem istnienia podstawy prawnej upoważniającej do przetwarzania przez nich danych osobowych, uczynić zadość zasadzie adekwatności. Adekwatność danych w stosunku do celu ich przetwarzania powinna być natomiast rozumiana jako równowaga pomiędzy dobrem osoby, której dane dotyczą, a interesem administratora danych.[207]

---

[204] DOLiS-72-12/13

[205] 1) imię i nazwisko lub nazwę właściciela nieruchomości oraz adres miejsca zamieszkania lub siedziby; 2) adres nieruchomości; 3) dane stanowiące podstawę zwolnienia z opłaty za gospodarowanie odpadami komunalnymi; 4) numer telefonu właściciela nieruchomości; 5) adres poczty elektronicznej właściciela nieruchomości; 6) inne informacje niezbędne do wystawienia tytułu wykonawczego

[206] Art. 7 pkt 4. Ilekroć w ustawie jest mowa o administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych

[207] Oznacza to, że administrator danych nie może przetwarzać danych w zakresie szerszym, niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem, stopniu szczegółowości. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w

Istotne jest także, by katalog danych, jakie mogą być zawarte we wzorze deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi był katalogiem zamkniętym – aby wykluczyć możliwość pozyskiwania danych w zakresie szerszym, niż jest to niezbędne ze względu na cel wynikający z ustawy. Kwestionowane rozwiązanie, tj. możliwość pozyskiwania za pośrednictwem deklaracji „innych informacji niezbędnych do wystawienia tytułu wykonawczego" stwarza ryzyko potencjalnych nadużyć. Przykładowo, niektóre gminy żądają od właścicieli nieruchomości udostępnienia w treści deklaracji informacji o miejscu zatrudnienia czy też danych dotyczących kont bankowych (np. pełny numer rachunku bankowego właściciela nieruchomości). Zbieranie tak szerokiego zakresu danych od wszystkich mieszkańców jedynie w celu ułatwienia egzekucji należności od osób, które nie wywiązują się z obowiązku uiszczenia opłaty za gospodarowanie odpadami komunalnymi stanowi nieproporcjonalną ingerencję w ich prywatność. Trudno przy tym uznać takie dane za „niezbędne do określenia wysokości opłaty za gospodarowanie odpadami komunalnymi".

Kwestionowane przepisy przewidywały również, że rada gminy może wymagać od właściciela nieruchomości podania jego numeru telefonu oraz adresu poczty elektronicznej. W praktyce, przedłożenie tych danych może zatem stać się obowiązkiem, zamiast wyłącznie możliwością. Powyższe pozostaje wątpliwe, albowiem w polskim porządku prawnym nie istnieje obowiązek posiadania telefonu czy poczty elektronicznej.

Niewątpliwie do prawidłowego wykonywania zadań wynikających z ustawy o utrzymaniu czystości i porządku w gminach może być konieczne pozyskiwanie stosownych informacji dotyczących właścicieli nieruchomości, jednak nie może dochodzić do sytuacji, w której to rada gminy, w sposób de facto dowolny, kształtować będzie zakres danych, jakie mogą być pozyskiwane od właścicieli nieruchomości. Konieczne jest zatem uspójnienie systemu na poziomie centralnym, tak, aby w przepisach ustawy zawarty został precyzyjny, zamknięty katalog danych osobowych, jakie mogą być przetwarzane.

W odpowiedzi z dnia 20 marca 2015 r. Ministerstwo Środowiska nie podzieliło zastrzeżeń Generalnego Inspektora, stwierdzając, iż gmina nie jest zobowiązana zawrzeć we wzorze deklaracji wszystkich wymienionych w ustawie danych, gdyż jest to katalog fakultatywny. To rada gminy, w drodze uchwały – mając na uwadze również zasady wynikające z ustawy o ochronie danych osobowych – ma decydować jakie informacje powinni podać właściciele nieruchomości.

---

jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane (wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r. o sygn. akt II SA/Wa 917/2005).

7) wystąpienie do Minister Edukacji Narodowej w sprawie umieszczania numeru PESEL na drukach legitymacji szkolnych

W związku z uwagami zgłaszanymi przez organ do spraw ochrony danych osobowych w toku uzgodnień międzyresortowych w trakcie prac nad nowelizacją rozporządzenia Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych(Dz. U. z 2014 r. poz. 893 z późn. zm.) oraz sygnalizowanymi Generalnemu Inspektorowi Ochrony Danych Osobowych wątpliwościami i zastrzeżeniami dotyczącymi konieczności umieszczania numeru PESEL ucznia na nowych wzorach legitymacji szkolnych (wzory nr 66a i 67a określone w załączniku nr 2 do rozporządzenia w sprawie świadectw, dyplomów państwowych i innych druków szkolnych), pismem z dnia 2 marca 2015 r. [208]organ do spraw ochrony danych osobowych zwrócił się o rozważenie wprowadzenia do rozporządzenia zmian dotyczących zakresu danych umieszczanych na legitymacji szkolnej.

Zasadniczym celem wydawania legitymacji szkolnych jest poświadczenie faktu uczęszczania ucznia do szkoły oraz jego uprawnienia do korzystania ze zniżek ustawowych przy przejazdach środkami publicznego transportu kolejowego i autobusowego i oba te cele były osiągane przez dotychczas zamieszczany zakres informacji o uczniu obejmujący jego imię, nazwisko, datę urodzenia i miejsce zamieszkania oraz oznaczenie szkoły, do której uczęszcza, zatem nie wydaje się, by do ich realizacji konieczne było rozszerzanie katalogu danych znajdujących się w treści legitymacji szkolnej. Wprawdzie projektodawca jako cel umieszczania na drukach numeru PESEL wskazał „dostosowanie wzorów legitymacji szkolnych do umożliwienia weryfikacji uprawnień w elektronicznym systemie potwierdzania uprawnień świadczeniobiorców (system e-WUŚ)", jednak wyłącznie na poziomie uzasadnienia do rozporządzenia w sprawie świadectw, dyplomów państwowych i innych druków szkolnych, nie zaś powszechnie obowiązujących przepisów.

Generalny Inspektor powołał się przy tym na art. 51 ust 2 Konstytucji RP oraz zasady celowości i adekwatności wynikające z przepisów ustawy o ochronie danych osobowych. Podkreślił jednocześnie, że dotychczas weryfikacja w systemie e-WUŚ była możliwa na podstawie legitymacji niezawierających numeru PESEL. Co istotne, polskie prawo gwarantuje bezpłatne świadczenia opieki zdrowotnej wszystkim dzieciom do ukończenia 18

[208] DOLiS-035-711/15

roku życia, tym bardziej więc nie jest uzasadnione zbyt rygorystyczne podejście do kwestii potwierdzania prawa do tych świadczeń przez osoby niepełnoletnie.

O ile zgodzić się należy, że zamieszczenie numeru PESEL w dokumencie może umożliwić weryfikację uprawnień w systemie e-WUŚ, dla którego jest to dana o zasadniczym znaczeniu, o tyle nie można się już zgodzić, aby takiemu celowi służyć miała legitymacja szkolna. Wskazać ponadto należy, że rozwiązanie prawne, na podstawie którego ujawniana ma być określona informacja i to w celu realizacji zadań innych podmiotów (tj. udzielania świadczeń opieki zdrowotnej uprawnionym do tego osobom) nie powinno wynikać z aktu o randze podustawowej, a tym bardziej – z rozporządzenia wydawanego na podstawie ustawy o systemie oświaty (w którym określone mają być m.in. warunki i tryb wydawania oraz wzory świadectw, dyplomów państwowych i innych druków szkolnych, sposób dokonywania sprostowań ich treści i wydawania duplikatów, a także tryb i sposób dokonywania legalizacji dokumentów przeznaczonych do obrotu prawnego z zagranicą), a zatem dotyczącego materii innej, niż świadczenia opieki zdrowotnej.

Generalny Inspektor Ochrony Danych Osobowych wskazał przy tym, że posługiwanie się numerem PESEL – będącym administracyjnym numerem identyfikacyjnym – jako podstawowym identyfikatorem w systemach zawierających informacje z zakresu ochrony zdrowia było przez niego poddawane w wątpliwość[209] – zwracał m.in. uwagę, że wykorzystywanie numeru PESEL w charakterze nazwy (loginu) osoby korzystającej z systemu informatycznego jest nieodpowiednie, gdyż stanowi zaprzeczenie podstawowych zasad bezpieczeństwa systemu informatycznego.

Mając na uwadze powyższe, w opinii organu do spraw ochrony danych osobowych, zachodziła potrzeba dokonania rzetelnej analizy zasadności umieszczania numeru PESEL ucznia na nowych wzorach legitymacji szkolnych, a w konsekwencji podjęcia prac nad zmianą stosownych przepisów prawa, zmierzających do usunięcia numeru PESEL ze wzoru i w konsekwencji z treści legitymacji szkolnej.

Pismem z dnia 11 maja 2015 r. Ministerstwo Edukacji Narodowej (załączając również stanowisko Ministerstwa Zdrowia) odniosło się do uwag GIODO, stwierdzając, iż wprowadzenie informacji o numerze PESEL ucznia na druku legitymacji szkolnej było

[209] Powołać można choćby stanowisko organu do spraw ochrony danych osobowych przedstawione do projektu rozporządzenia Ministra Zdrowia w sprawie sposobu identyfikacji usługobiorców, pracowników medycznych i usługodawców oraz sposobu i trybu przekazywania przez usługodawców informacji o pracownikach medycznych udzielających świadczeń opieki zdrowotnej na rzecz usługobiorców(wydawanego na podstawie delegacji zawartej w art. 18 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia – Dz. U. Nr 113, poz. 657 z późn. zm.).

działaniem merytorycznie uzasadnionym oraz uprawnionym biorąc pod uwagę mechanizm potwierdzania prawa świadczeniobiorcy do świadczeń opieki zdrowotnej na podstawie dokumentu elektronicznego generowanego z systemu e-WUŚ.

8) wystąpienie do Ministra Infrastruktury i Rozwoju dotyczące przetwarzania danych osobowych osób ubiegających się o najem lokali należących do mieszkaniowego zasobu gminy

Pismem z dnia 2 marca 2016 r.[210]organ do spraw ochrony danych osobowych zwrócił się o rozważenie wprowadzenia do ustawy z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego (Dz. U. z 2014 r. poz. 150 z późn. zm.) przepisów regulujących kwestie związane z przetwarzaniem danych osobowych.

W związku z sygnalizowanymi Generalnemu Inspektorowi Ochrony Danych Osobowych wątpliwościami i zastrzeżeniami dotyczącymi stosowania przepisów ustawy organ wskazał, że obecne regulacje w niej zawarte mogą prowadzić do nadmiernej ingerencji w prywatność osób ubiegających się o najmem lokali. Zgodnie z art. 21 ust. 1 pkt 1 ustawy, określenie zasad wynajmowania lokali wchodzących w skład mieszkaniowego zasobu gminy ma miejsce w drodze uchwały rady gminy. Art. 21 ust. 3 wskazuje zaś, jakie kwestie powinny w szczególności określać te zasady[211]. W opinii Generalnego Inspektora, duży stopień ogólności tych przepisów stwarza ryzyko potencjalnych nadużyć dotyczących zakresu danych osobowych, jakie mogą być pozyskiwane przez gminę. Niewątpliwie do prawidłowego gospodarowania zasobem mieszkaniowym gminy konieczne jest pozyskiwanie stosownych informacji od osób, które są zainteresowane najmem mieszkania z tego zasobu, co jest równoznaczne z przetwarzaniem ich danych osobowych. Należy jednak mieć na uwadze, iż z uwagi na specyfikę komentowanej ustawy, mogą to by również tzw. dane szczególnie

[210] DOLiS-035-712/15

[211] 1) wysokość dochodu gospodarstwa domowego uzasadniającą oddanie w najem lub w podnajem lokalu na czas nieoznaczony i lokalu socjalnego, oraz wysokość dochodu gospodarstwa domowego uzasadniającą zastosowanie obniżek czynszu; 2) warunki zamieszkiwania kwalifikujące wnioskodawcę do ich poprawy; 3) kryteria wyboru osób, którym przysługuje pierwszeństwo zawarcia umowy najmu lokalu na czas nieoznaczony i lokalu socjalnego; 4) warunki dokonywania zamiany lokali wchodzących w skład mieszkaniowego zasobu gminy oraz zamiany pomiędzy najemcami lokali należących do tego zasobu a osobami zajmującymi lokale w innych zasobach; 5) tryb rozpatrywania i załatwiania wniosków o najem lokali zawierany na czas nieoznaczony i o najem lokali socjalnych oraz sposób poddania tych spraw kontroli społecznej; 6) zasady postępowania w stosunku do osób, które pozostały w lokalu opuszczonym przez najemcę lub w lokalu, w którego najem nie wstąpiły po śmierci najemcy;7) kryteria oddawania w najem lokali o powierzchni użytkowej przekraczającej 80 m^2.

chronione (wrażliwe), np. dotyczące stanu zdrowia, czy orzeczeń wydanych w sprawie konkretnej osoby.

Zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych przetwarzanie danych o statusie „szczególnie chronione" jest co do zasady zabronione. Zasada ta doznaje wyjątków jedynie w przypadkach enumeratywnie wymienionych w art. 27 ust. 2 ustawy. Tymczasem żaden z przepisów ustawy o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego nie odnosi się wprost do kwestii pozyskiwania danych osobowych na potrzeby realizacji zadania polegającego na wynajmowaniu lokali wchodzących w skład zasobu mieszkaniowego gminy. Stosowne ustalenia w tym zakresie pozostawione zostały radzie gminy, która w drodze uchwały określa zasady wynajmowania lokali wchodzących w skład mieszkaniowego zasobu gminy, nie posiadając de facto podstawy prawnej w postaci przepisów ustawy, które zezwalałyby na pozyskiwanie i dalsze przetwarzanie określonego zakresu danych osobowych, jak i określały ich zakres czy sposoby przetwarzania, w tym okresy przechowywania. W opinii Generalnego Inspektora rozwiązanie takie stoi w sprzeczności z orzecznictwem Trybunału Konstytucyjnego[212].

Rozumiejąc zatem potrzebę pozyskiwania danych osobowych, organ wskazał, że nie może się ono odbywać na zasadzie pełnej dowolności. Tymczasem, z sygnałów docierających do Generalnego Inspektora Ochrony Danych Osobowych wynika, iż praktyki poszczególnych gmin związane z pozyskiwaniem informacji na temat osób starających się o najmem mieszkania z zasobu gminy znacząco się różnią[213]. Konieczne jest zatem uspójnienie systemu na poziomie centralnym, tak, aby zakres danych osobowych, jakie mogą być przetwarzane

[212] Zgodnie ze stanowiskiem Trybunału Konstytucyjnego, wyrażonym w postanowieniu z dnia 31 stycznia 2007 r. (sygnatura S 1/2007), „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". Wymóg umieszczenia bezpośrednio w ustawie wszystkich zasadniczych elementów regulacji prawnej musi być stosowany ze szczególnym rygoryzmem, gdy regulacja ta dotyczy korzystania przez obywateli z ich praw i wolności (wyrok Trybunału Konstytucyjnego z dnia 25 maja 1998 r. sygnatura U 19/97). Podobnie orzekł Trybunał w wyroku z dnia 18 grudnia 2014 r. (sygnatura K 33/13), dotyczącym tworzenia rejestrów danych medycznych na podstawie rozporządzenia przez ministra zdrowia.

[213] Przykładowo, ubieganie się o najem lokalu z mieszkaniowego zasobu m.st. Warszawy wymaga podania szczegółowych danych dotyczących nie tylko wnioskodawcy, ale także współmałżonka wnioskodawcy i innych osób ubiegających się wspólnie z nimi o najem. Ponadto, w stosownym wniosku należy podać szczegółowe informacje dotyczące obecnych warunków mieszkaniowych, stanu majątkowego, uzyskiwanych dochodach, stanu zadłużenia, pobieranych zasiłkach, ewentualnych przewlekłych chorób lub niepełnosprawności oraz sytuacji rodzinnej i osobistej (uzależnienie, przemoc). Dane te dotyczą zarówno wnioskodawcy, jego współmałżonka, jak i wszystkich innych osób, które miałyby zamieszkiwać w lokalu (a więc także dzieci). Tak szeroki zakres informacji zawierających również dane szczególnie chronione (w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych), nie może być przetwarzany bez podstawy w prawnej wyrażonej w akcie prawa powszechnie obowiązującego, jak i gwarantującej pełną ich ochronę.

wynikał wprost z przepisów ustawy – tym bardziej z uwagi na fakt, iż w celu realizacji zadań wynikających z komentowanej ustawy dochodzić będzie również do przetwarzania danych wrażliwych.

Generalny Inspektor przypomniał przy tym, iż prawo do ochrony prywatności i prawo do ochrony danych osobowych są prawami osobistymi gwarantowanymi przez Konstytucję Rzeczypospolitej Polskiej (art. 47 i art. 51), a więc ograniczenie w zakresie korzystania z tych praw wymaga regulacji rangi ustawowej. Dodatkowo, oparcie każdej formy przetwarzania danych osobowych jednostki na przepisie prawa jest obowiązkiem podmiotów publicznych, albowiem organy publiczne obowiązane są do działania jedynie na podstawie i w granicach prawa (zasada legalizmu - art. 7 Konstytucji RP oraz art. 6 Kodeksu postępowania administracyjnego). Granice działań podmiotów publicznych wyznaczają wyłącznie normy prawne określające ich kompetencje, zadania i tryb postępowania.

Za uzupełnieniem przepisów ustawy o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego przemawiają również zasady legislacji, w szczególności, wynikająca z §132 w zw. z §25 ust. 1 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. Nr 100, poz. 908), która nakazuje tworzenie przepisów precyzyjnych, umożliwiających wywiedzenie, kto, w jakich okolicznościach i jak powinien się zachować oraz zasada adekwatności wynikająca z 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Mając powyższe na uwadze, Generalny Inspektor wystąpił o podjęcie prac nad zmianą stosownych przepisów prawa i stworzenie regulacji precyzyjnie określających zasady przetwarzania danych osobowych osób ubiegających się o najem mieszkania z zasobu gminy. Konieczne jest zwłaszcza stworzenie precyzyjnego, zamkniętego katalogu danych, jakie mogą być pozyskiwane.

Ministerstwo Infrastruktury i Rozwoju w odpowiedzi na wystąpienie z dnia 27 marca 2015 r. stwierdziło, iż istniejące przepisy prawne przewidują wystarczające środki ochrony danych osobowych, a tym samym nie ma podstaw do podjęcia inicjatywy legislacyjnej.

9) wystąpienie do Zakładu Karnego w związku z bezpodstawnym pozyskiwaniem szerokiego zakresu danych osobowych poprzez pozyskiwanie i archiwizowanie kopii dowodów tożsamości osób odwiedzających osadzonych

Pismem z dnia 28 września 2015 r.[214] Generalny Inspektor Ochrony Danych Osobowych wystosował, na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych, do jednego z Zakładów Karnych wystąpienie w związku z praktyką polegającą na przetwarzaniu danych osobowych osób odwiedzających osadzonych za pomocą pozyskiwania kopii dokumentów potwierdzających tożsamość. Generalny Inspektor Ochrony Danych Osobowych wskazał, iż taka praktyka nie jest zgodna z przepisami prawa.

Organ do spraw ochrony danych osobowych w ww. wystąpieniu podniósł, iż podmioty przetwarzające dane zarówno pozyskując je, jak i żądając ich udostępnienia powinny wskazywać podstawę prawną wykonywania operacji na danych osobowych w postaci przepisów szczególnych regulujących ich działalność, zwłaszcza gdy związane są stosownymi normami kompetencyjnymi, wyznaczającymi zakres ich działania. Generalny Inspektor wskazał również, iż cel i zakres przetwarzania danych osobowych przez podmioty publiczne, jest najczęściej wyznaczony przepisami prawa i wynika on bezpośrednio z określonych prawem zadań danego podmiotu[215].

Generalny Inspektor powołując się na art. 51 Konstytucji RP wskazał, iż nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby (ust. 1). Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (ust. 2). Ponadto zaś, zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa (ust. 5)[216].

Organ do spraw ochrony danych jednocześnie przypomniał, iż kopiowanie dokumentów jest czynnością techniczną, która ze swojej istoty nie jest zakazana przepisami ustawy o ochronie danych osobowych. Z punktu widzenia przepisów ustawy istotne jest jednak, aby podmiot, który dokonuje takiej czynności, legitymował się jedną z przesłanek legalności przetwarzania, w tym gromadzenia danych osobowych, które dla danych tzw. zwykłych (np.

[214] DOLiS-035-123/15

[215] Stosownie do postanowienia Naczelnego Sądu Administracyjnego z dnia 16 grudnia 2004 r. (sygn.: FSK 417/2004) „*Normy kompetencyjnej nie można domniemywać i nie można jej konstruować w procesie wykładni prawa. Musi być ona wyraźnie w ustawie określona, nigdy nie można przyjmować zasady domniemania kompetencji publicznoprawnej, jeżeli przepisy ustawowe w tym względzie milczą*".

[216] Por. wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. (sygn. K 32/2004) „*konieczność w demokratycznym państwie prawnym to zastosowanie środków niezbędnych (koniecznych) w tym sensie, że będą one chronić określone wartości w sposób lub stopniu, który nie mógłby być osiągnięty pry zastosowaniu innych środków, a jednocześnie winny to być środki jak najmniej uciążliwe dla podmiotów, których prawo lub wolność ograniczają*".

imię, nazwisko, adres zameldowania) określone zostały w art. 23 ust. 1, zaś danych tzw. wrażliwych w art. 27 ust. 2 ustawy o ochronie danych osobowych, oraz aby kopiowanie dokumentów nie prowadziło do gromadzenia danych w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są przetwarzane (art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych)[217]. W związku z powyższym, dane osobowe muszą być przetwarzane zgodnie z zasadą adekwatności, która stanowi, iż dane swym rodzajem i treścią nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania. Administrator danych nie może przetwarzać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem stopień szczegółowości. Wątpliwości GIODO wzbudziła również kwestia sposobu i okresu przechowywania pozyskanych danych.

W opinii Generalnego Inspektora dane zawarte w kopii dokumentu tożsamości są pozyskiwane bez stosownej podstawy prawnej, a tym samym przetwarzane niezgodnie z prawem. W związku z powyższym, Generalny Inspektor zwrócił się do dyrektora Zakładu Karnego o zaprzestanie stosowania praktyki polegającej na pozyskiwaniu danych osobowych osób odwiedzających osadzonych za pomocą kopii ich dokumentów potwierdzających tożsamość.

Pismem z dnia 20 października 2015 r. dyrektor Zakładu Karnego poinformował, że praktyka pozyskiwania kopii dokumentów potwierdzających tożsamość została zaprzestana wraz z początkiem 2015 r., na polecenie Dyrektora Okręgowego Służby Więziennej.

10) wystąpienie do placówki bankowej w związku z podawaniem nieistniejących podstaw prawnych dotyczących zgody na przetwarzanie danych osobowych oraz jednoczesnego wymuszania od klientów tych zgód

Generalny Inspektor w dniu 28 września 2015 r.[218], wystosował wystąpienie do prezesa zarządu jednego z banków, po pozyskaniu informacji, iż przedmiotowy bank stosuje praktykę wprowadzania w błąd osób kontaktujących się z bankiem przez stronę internetową poprzez

[217] Stosownie do wyroku Naczelnego Sądu Administracyjnego z dnia 19 grudnia 2001 r. (sygn. II SA 2869/00) *„gromadzenie danych osobowych przez wykonanie kopii dokumentu zawierającego te dane jest kwestią techniczną, obojętną dla prawodawcy reglamentującego w ustawie o ochronie danych osobowych przetwarzanie tego rodzaju danych. Inaczej mówiąc posługiwanie się taką czy inną techniką utrwalania danych (kopiowanie lub przepisywanie) nie przesądza samo przez się o legalności albo nielegalności tego utrwalania (przetwarzania). Dla takich ocen istotne znaczenie mają przede wszystkim: podstawa prawna przetwarzania danych (art. 23 ustawy), rodzaj przetwarzanych danych (art. 27) oraz granice przetwarzania (art. 26 ust. 1 pkt 3)*". Analogiczne stanowisko zajął Naczelny Sąd Administracyjny w wyroku z dnia 7 listopada 2003 r. (sygn. akt II SA 1432/02) *„ustawa o ochronie danych osobowych nie zajmuje się określaniem techniki gromadzenia danych osobowych lecz zakresem ich przetwarzania (...)"*

[218] DOLiS-035-304/15

wymuszanie zgód na przetwarzanie danych osobowych w bliżej nieokreślonym celu oraz informowanie o istnieniu „podstaw prawnych" faktycznego wymuszania ww. zgody.

Organ do spraw ochrony danych osobowych wskazał, iż osoba kontaktująca się z bankiem za pośrednictwem strony internetowej nie ma możliwości skutecznego kontaktu bez wyrażenia ww. „zgody". Dodatkowo przepis, który wskazał bank (art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych) nie stanowi o uprawnieniu banku do pozyskania (wymuszenia) zgody, lecz o prawie osoby, której dane dotyczą, do wyrażenia jej dobrowolnie.

Zdaniem Generalnego Inspektora opisana wyżej praktyka budzi zastrzeżenia w kontekście zasad, które wynikają z przepisów ustawy o ochronie danych osobowych, a w szczególności w kontekście określonej ustawą definicji zgody na przetwarzanie danych osobowych. Jednocześnie organ wskazał, iż z definicji tej nie wynikają szczegółowe zasady formułowania zgody, jednakże z treści zgody na przetwarzanie danych osobowych powinno w sposób nie budzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Generalny Inspektor oparł się również na literaturze przedmiotu, w której podkreśla się, iż zgoda nie powinna mieć charakteru abstrakcyjnego, nie może dotyczyć przetwarzania danych osobowych „w ogóle", czyli nie może też przybierać formy użytej przez bank, tj. przetwarzania „w szczególności w celach marketingowych". Chodzi zatem o to, by odnosiła się ona do skonkretyzowanego stanu faktycznego, obejmowała tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania[219]. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi[220].

W swoim wystąpieniu organ do spraw ochrony danych osobowych podkreślił, iż zgoda na przetwarzanie danych osobowych powinna być udzielana dobrowolnie. Wskazał, iż praktyka banku stosowana na stronie internetowej przez akceptację klauzuli zgody na przetwarzanie danych osobowych „w szczególności w celach marketingowych" w praktyce zezwala na pełną dowolność kontaktu banku z osobą, która wyraziła tę zgodę. Osoba ma prawo nie godzić się na uzależnianie zawarcia umowy od wyrażenia zgody na przetwarzanie danych osobowych w bliżej nieokreślonych celach marketingowych. Zgoda powinna spełniać wskazane wyżej wymogi i może być udzielona jedynie dobrowolnie, a zatem powinna być zapewniona tzw. opcjonalność jej wyrażenia.

[219] J. Barta. P. Fajgielski, R. Markiewicz, *Ochrona Danych Osobowych. Komentarz*, Zakamycze 2004, s. 420

[220] por. wyrok NSA z dnia 4 kwietnia 2003 r. o sygn. akt II SA 2135/2002, czy też wyrok NSA z dnia 11 kwietnia 2003 r. o sygn. akt: II SA 3942/2004

Generalny Inspektor podniósł również, iż zgoda wyrażana na podstawie art. 10 ust. 2 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 z późn. zm.) jako ściśle związana z przetwarzaniem danych osobowych, również powinna być gromadzona w sposób, który zapewnia realizację prawa osoby, której dane dotyczą.[221] Dodatkowo wskazaniu podlegał także fakt, iż na gruncie ustawy o ochronie danych osobowych dopuszczalność przetwarzania, w tym gromadzenia danych osobowych tzw. zwykłych uzależniona jest od spełnienia jednej z przesłanek wymienionych w art. 23 ust. 1 pkt 1-5 ustawy o ochronie danych. Spełnienie jednej z tych przesłanek czyni proces przetwarzania danych legalnym. Jeżeli przetwarzanie danych nie spełnia żadnej z pozostałych przesłanek legalności, wtedy należy uzyskać zgodę osoby, której dane są przetwarzane.[222] Dodatkowo należy wskazać, iż czym innym jest pozyskanie zgody na przetwarzanie danych, a czym innym spełnienie obowiązku informacyjnego[223].

W wymaganym 30-dniowym terminie do ustosunkowania się do niniejszego wystąpienia, bank poinformował, iż formularz służący do kontaktowania się z bankiem został

[221] Podobne stanowisko:. Kasprzycki, *Spam...*, s. 61-69; G. Rączka, *Ochrona usługobiorcy...*, s. 107; zob. też uwaga 2 do art. 4 u.ś.u.d.e., Chomiczewski W.; Klafkowska-Waśniowska K.; Lubasz D. (red.); Namysłowska M. (red.); Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw, LexisNexis Polska, 2011; *„Kwestia braku zamówienia informacji handlowej przybliżona została w art. 10 ust. 2 u.ś.u.d.e., zgodnie z którym informacja handlowa jest zamówiona, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny. Konieczność wyrażenia uprzedniej zgody jest wyrazem przyjęcia tzw. modelu opt-in, który w większym stopniu chroni interesy potencjalnego usługobiorcy usług świadczonych drogą elektroniczną. Przeciwne rozwiązanie, tzw. model opt-out, wymaga bowiem zaangażowania odbiorcy w formie wyrażenia sprzeciwu wobec otrzymywania informacji handlowych i nie zapobiega otrzymywaniu pierwszej niezamówionej informacji handlowej*". Przy czym, art. 4 ust. 1 ustawy o świadczeniu usług drogą elektroniczną stanowi, że jeżeli ustawa wymaga uzyskania zgody usługobiorcy, to zgoda ta: 1) nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; 2) może być odwołana w każdym czasie. Zatem zasadnym jest postulowanie, aby wyrażenie takiej zgody miało charakter w pełni dobrowolny zwłaszcza, iż zgodnie z art. 16 ust. 1 ustawy o świadczeniu usług drogą elektroniczną do przetwarzania danych osobowych w rozumieniu ustawy o ochronie danych osobowych, w związku ze świadczeniem usług drogą elektroniczną, stosuje się przepisy tej ustawy (o ile przepisy rozdziału 4 ustawy o świadczeniu usług drogą elektroniczną nie stanowią inaczej).

[222] Art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych.

[223] Art. 24-25 ustawy o ochronie danych osobowych. Dopełnienie przez administratora danych przedmiotowego obowiązku powinno polegać na rzetelnym przekazaniu informacji odnoszących się do wszystkich elementów określonych w art. 24 ust. 1 pkt 1 - 4 ustawy o ochronie danych osobowych, chyba, że zachodzą przesłanki wyłączające obowiązek jego wypełnienia, przewidziane w art. 24 ust. 2 i art. 25 ust. 2 ustawy. W tej sprawie szczególne znaczenie mają przepisy art. 24 ustawy, zgodnie z którym, *administrator danych winien wypełnić obowiązek informacyjny wobec osób, których dane pozyskuje bezpośrednio od tych osób,*
i poinformować te osoby 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. Stosownie zaś do treści art. 24 ust. 2 ustawy, *z powyższego obowiązku administrator danych jest zwolniony jeżeli: 1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania, 2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1*.

natychmiast poprawiony, a poprzednio wymagane pola zostały usunięte wraz z błędną informacją o istniejącej podstawie prawnej w tym zakresie.

11) wystąpienie do burmistrza miasta w sprawie rozsyłania korespondencji w formie obejmującej rozdzielnik zawierający dane osobowe w postaci imion i nazwisk oraz adresów osób fizycznych

Generalny Inspektor w dniu 4 listopada 2015 r.[224] skierował do burmistrza jednego z miast wystąpienie dotyczące rozsyłania korespondencji w formie obejmującej rozdzielnik zawierający dane osobowe w postaci imion i nazwisk oraz adresów osób fizycznych.

Organ do spraw ochrony danych osobowych zwrócił uwagę, iż takie działanie jest niczym nie poparte oraz budzi sprzeciw osób, które znajdują się na liście adresatów. Generalny Inspektor wskazał jednocześnie, iż w przypadku rozsyłania pism o zbiorczym charakterze wydaje się zasadne, aby dane osobowe wszystkich adresatów zamieszczone były na odrębnej karcie (rozdzielniku), która pozostaje jedynie w dyspozycji organu, a pisma rozsyłane były następnie indywidualnie do każdej z zainteresowanych osób, bez przesyłania każdej z nich listy imion, nazwisk i adresów pozostałych osób. Generalny Inspektor wskazał również, iż na każdym administratorze danych ciąży obowiązek przetwarzania danych zgodnie z zasadami, które wynikają z przepisów prawa, w tym ustawy o ochronie danych osobowych[225].

Organ do spraw ochrony danych osobowych podkreślił jednocześnie, iż naruszanie zasad, które wynikają z ustawy o ochronie danych osobowych może skutkować zarówno odpowiedzialnością administracyjną, jak i karną - przed Generalnym Inspektorem Ochrony Danych Osobowych i organami właściwymi do ścigania przestępstw.

Burmistrz miasta na niniejsze wystąpienie odpowiedział w dniu 30 listopada 2015 r., wskazując iż w wyniku przeprowadzonego postępowania wyjaśniającego ustalono, iż doszło do pojedynczego rozesłania korespondencji wraz z rozdzielnikiem zawierającym dane osobowe adresatów. Wskazał, iż taka sytuacja wystąpiła jednorazowo i wynikała z niewiedzy

[224] DOLiS-035-555/15

[225] Zgodnie z przesłankami wskazanymi w art. 23 ust.1 pkt 1-5 ustawy o ochronie danych osobowych, oraz gdy przetwarzanie danych osobowych dotyczy danych tzw. „wrażliwych" – zgodnie z art. 27 ust. 2 pkt 1-10 ustawy o ochronie danych osobowych. Stosując w swej działalności zasady ochrony danych osobowych administrator danych, powinien dopełniać obowiązku dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt 1-4 ustawy o ochronie danych osobowych).

pracownika urzędu miasta. Pracownik ten został pouczony o konieczności przestrzegania procedur dotyczących ochrony danych osobowych, natomiast w samym urzędzie zaplanowano przeprowadzenie dodatkowych szkoleń pracowników, które mają na celu zwrócenie uwagi na kwestie zamieszczania danych osobowych w pismach kierowanych do wielu stron postępowania. Dodatkowo burmistrz wskazał, iż w urzędzie jest wprowadzona zarządzeniem burmistrza polityka bezpieczeństwa.

12) wystąpienie do Ministra Spraw Wewnętrznych z wnioskiem o podniesienie wśród wojewodów problemu niezgodnego z przepisami prawa przetwarzania (pozyskiwania) danych osobowych przez straże miejskie

Na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych Generalny Inspektor skierował do Ministra Spraw Wewnętrznych wystąpienie w dniu 28 lipca 2015 r.[226], z uwagi na ogromną ilość sygnałów od osób fizycznych oraz przedsiębiorców dotyczących problemu przetwarzania danych osobowych przez straże gminne niezgodnie z prawem – bez stosownej ku temu podstawy prawnej i w zakresie nieadekwatnym do celu ich przetwarzania[227].

Sygnały te dotyczyły stosowania przez straże gminne formularzy za pomocą których pozyskiwane są dane osobowe.[228] Formularze te obejmują zbieranie danych tzw. „szczególnie chronionych" zgodnie z art. 27 ust. 1 ustawy o ochronie danych osobowych, których przetwarzanie jest zabronione, o ile nie jest spełniona jedna z przesłanek legalności wskazanych w art. 27 ust. 2 ustawy o ochronie danych osobowych.

Generalny Inspektor wskazał, iż rozumie, że realizacja przez straż gminną zadań nałożonych na nią ustawowo wymaga wykorzystywania informacji o osobach, których działania te dotyczą. Przepisy ustawy o strażach gminnych wprost stanowią o prawie straży gminnej do przetwarzania danych w związku z realizacją określonych prawem zadań, bez konieczności uzyskania na to zgody osoby, której dane dotyczą. Zakres jednak przetwarzanych przez straże miejskie danych osobowych w wielu sygnalizowanych

[226] DOLiS-035-2499/15

[227] Mocą przepisów ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23) w związku z przepisami ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2016 r., poz. 543), zakres kompetencji Ministra Spraw Wewnętrznych obejmuje m.in. nadzór nad działalnością wojewodów w dziale sprawy wewnętrzne dotyczące ochrony bezpieczeństwa i porządku publicznego, wojewodowie zaś mocą przepisów ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 2013 r. poz. 1383 z późn. zm.) sprawują nadzór nad działalnością straży gminnych przy pomocy komendantów wojewódzkich (w tym Stołecznego) Policji działających w ich imieniu

[228] W szczególności wykonując zadania w zakresie kontroli ruchu drogowego, o których mowa w art. 129b ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym (Dz. U. z 2012 r. poz. 1137 z późn. zm.), jak i w zakresie utrwalania przesłuchań.

przypadkach jest nieadekwatny do celu ich przetwarzania, naruszając tym samym przepisy prawa.[229]

W wystąpieniu Generalny Inspektor odniósł się do przykładów formularzy służących do realizacji zadań straży gminnych, w tym w szczególności dotyczących nakładania grzywien w postępowaniu mandatowym za wykroczenia, czy dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych – w trybie i zakresie określonym w Kodeksie postępowania w sprawach o wykroczenia[230].

Organ do spraw ochrony danych osobowych otrzymał informację, iż np. w protokołach przesłuchań osób podejrzanych o wykroczenia pojawiają się rubryki rodzaju „narodowość", co w świetle art. 10a ustawy o strażach gminnych jest niedopuszczalne[231].

Generalny Inspektor wskazał, iż przetwarzanie danych osobowych musi odbywać się zgodnie z zasadami określonymi w art. 26 ust. 1 ustawy o ochronie danych osobowych[232]. Między innymi, dane osobowe muszą być przetwarzane zgodnie z zasadą adekwatności. Zasada ta oznacza, iż dane swym rodzajem i treścią nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania. Administrator danych nie może więc przetwarzać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem stopniu szczegółowości. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to

[229] Stosownie do brzmienia art. 12 ust. 1 pkt 5 ustawy o strażach gminnych, strażnik wykonując zadania, o których mowa w art. 10 i 11, ma prawo do dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych – w trybie i zakresie określonych w przepisach ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. 2013 r. poz. 395 z późn. zm.). Straż gminna jest bowiem jednym z oskarżycieli publicznych w myśl art. 17 Kodeksu postępowania w sprawach o wykroczenia, któremu przysługuje prawo do zebrania danych niezbędnych do sporządzenia wniosku o ukaranie (art. 54 – 56 ustawy Kodeks postępowania w sprawach o wykroczenia). Zakres tych danych jednakże określony jest w art. 57 § 1 ustawy Kodeks postępowania w sprawach o wykroczenia, mianowicie w art. 57 § 2 i 3, i nie może być on kreowany swobodnie, czy też usprawiedliwiany np. tym, iż „określony wzór protokołu, w którym jedną z rubryk była narodowość, funkcjonował (…) od kilku lat" (cyt. z protokołu kontroli jednego z wojewodów).

[230] Nieuzasadnionym np. jest: przetwarzanie przez straże miejskie danych dotyczących nazwisk rodowych (ewentualnie nazwiska panieńskiego), imion rodziców, miejsca urodzenia, zwłaszcza w sytuacji, gdy pozyskiwany jest nr PESEL – tj. zgodnie z art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2015 r. poz. 388, z późn. zm.) jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną.

[231] Zgodnie z art. 10a ustawy o strażach gminnych, w celu realizacji zadań straż może przetwarzać dane osobowe, jednak – co należy podkreślić - z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym (tj. danych, o których mowa w art. 27 ust. 1 ustawy), bez wiedzy i zgody osoby, której dane te dotyczą uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia.

[232] Vide przypis nr 6.

niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane[233]. Jeżeli administrator uzurpuje sobie więcej praw niż przewidują obowiązujące przepisy prawa, następuje zachwianie równowagi na korzyść administratora, a zatem ma miejsce bezpodstawne ograniczenie praw osoby, której dane dotyczą, i – *de facto* – następuje przetwarzanie danych bez podstawy prawnej.

Niniejszym wystąpieniem Generalny Inspektor zasygnalizował konieczność podjęcia działań niwelujących zaistniałe w strażach miejskich nieprawidłowości. Dobrym - zdaniem organu do spraw ochrony danych osobowych - środkiem naprawczym w tym zakresie, byłoby uwidocznienie tej sprawy wojewodom.[234] Tym samym za pomocą środków, którymi wojewodowie posługują się na co dzień, możliwym jest osiągnięcie wnioskowanych w wystąpieniu rezultatów.

Pismem z dnia 3 września 2015 r. Minister Spraw Wewnętrznych podzielił stanowisko GIODO przekazując jego wystąpienie organom, które sprawują nadzór nad strażami gminnymi: wójtom, burmistrzom, prezydentom miast. W piśmie tym MSW wskazało, iż kontrola gromadzenia i przetwarzania danych osobowych, powinna być prowadzona przez właściwy organ, w zakresie jego ustawowych uprawnień.

13) wystąpienie do Ministra Spraw Wewnętrznych w sprawie podjęcia działań legislacyjnych mających na celu zapewnienie strażom gminnym dostęp do danych objętych tajemnicą telekomunikacyjną w zakresie, w jakim jest to niezbędne do przeprowadzenia czynności wyjaśniających

Generalny Inspektor w dniu 28 lipca 2015 r. wystąpił z pismem do Ministra Spraw Wewnętrznych[235] z wnioskiem o podjęcie działań legislacyjnych zmierzających do znowelizowania przepisów ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 2013 r. poz. 1383, z późn. zm.), prowadzącego do zapewnienia strażom gminnym dostępu do

[233] Podobnie wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r. (sygn. akt II SA/Wa 917/2005).

[234] Wojewoda bowiem, działając w oparciu o przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia z dnia 21 grudnia 2009 r. w sprawie trybu sprawowania nadzoru nad działalnością straży gminnych (miejskich) (Dz. U. z 2009 r. Nr 220 poz. 1733 z późn. zm.) w porozumieniu z komendantem wojewódzkim (Stołecznym) Policji sporządza plan kontroli okresowych na rok kalendarzowy, zawierający m.in. zakres (tematykę) kontroli, w którym można by uwzględnić szczególny nacisk na procesy przetwarzania, w tym pozyskiwania danych osobowych za pomocą formularzy (§ 3 ww. rozporządzenia). Podczas wykonywania czynności kontrolnych przez kontrolującego mogą być obecni przedstawiciele wojewody (posiadający pisemne upoważnienie wojewody § 5). Co najistotniejsze natomiast, po zakończeniu kontroli kontrolujący sporządza projekt wystąpienia pokontrolnego zawierającego informacje o wynikach kontroli, a w przypadku pojawienia się uwag i wniosków z niej wynikających - także zalecenia zmierzające do usunięcia stwierdzonych uchybień oraz termin na wykonanie wydanych zaleceń, który wojewoda przekazuje m.in. kierownikowi jednostki kontrolowanej (§ 11).

[235] DOLiS-035-2498/15

danych objętych tajemnicą telekomunikacyjną w zakresie, w jakim jest im to niezbędne do przeprowadzenia czynności wyjaśniających w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych - zgodnie z art. 12 ust. 1 pkt 5 ustawy o strażach gminnych i art. 17 § 3 i 54 - 57 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. 2013 r. poz. 395 z późn. zm.).

Zdaniem Generalnego Inspektora istniejące przepisy w obecnym brzmieniu i zakresie utrudniają ich rozumienie przedsiębiorcom telekomunikacyjnym i powodują rozbieżności interpretacyjne utrudniające realizowanie przez właściwe organy obowiązków wynikających z przepisów prawa. Dotyczy to zwłaszcza straży gminnych strzegących przecież porządku publicznego i egzekwujących przepisy prawa w granicach przyznanych im kompetencji. Celem egzekwowania prawa jest nałożenie sankcji karnej na osobę, która łamie przepisy, ku czemu niezbędne jest efektywne zebranie niezbędnych informacji zmierzających do ukarania sprawcy.[236] Straż gminna, zdaniem organu do spraw ochrony danych osobowych, posiada podstawę prawną do pozyskania danych osobowych na mocy ww. przepisów prawa[237].

[236] Praktyka działalności organu do spraw ochrony danych osobowych dowodzi, iż przedsiębiorcy telekomunikacyjni w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2014 r. poz. 243 z późn. zm.), odmawiają udostępnienia informacji stanowiących tajemnicę telekomunikacyjną - powołując się na uregulowania ww. ustawy. W takich przypadkach, straże miejskie składają skargi do Generalnego Inspektora Ochrony Danych Osobowych, aby ten, korzystając ze swych – przewidzianych przepisami ustawy o ochronie danych osobowych – uprawnień, nakazał określonemu przedsiębiorcy telekomunikacyjnemu udostępnienie straży miejskiej danych osobowych. Taki stan rzeczy powoduje w wielu przypadkach wydłużanie postępowań prowadzonych przez straże miejskie, a przede wszystkim prowadzenie postępowań, których można by uniknąć, w przypadku organu do spraw ochrony danych osobowych. W konsekwencji dochodzić może do podważania zasad określonych w przepisach Kodeksu postępowania administracyjnego, chociażby jej art. 12 § 1 stanowiącego, iż organy administracji publicznej powinny działać w sprawie wnikliwie i szybko, posługując się możliwie najprostszymi środkami prowadzącymi do jej załatwienia, czy art. 8 stanowiącego, że organy administracji publicznej prowadzą postępowanie w sposób budzący zaufanie jego uczestników do władzy publicznej.

[237] Zgodnie z art. 10 ust. 1 ustawy o strażach gminnych, straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. W celu realizacji tych zadań straż może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia (art. 10a pkt 1 ustawy o strażach gminnych). Stosownie do brzmienia art. 12 ust. 1 pkt 5 ustawy o strażach gminnych, strażnik wykonując zadania, o których mowa w art. 10 i 11, ma prawo do dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych – w trybie i zakresie określonych w Kodeksie postępowania w sprawach o wykroczenia. Dodatkowo zgodnie z art. 17 kodeksu postępowania w sprawach o wykroczenia, któremu przysługuje prawo do przeprowadzenia czynności wyjaśniających w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie (art. 54 – 56 ustawy Kodeks postępowania w sprawach o wykroczenia). Zwrócić należy uwagę, iż w myśl art. 54 ust. 1 *in fine* ustawy Kodeks postępowania w sprawach o wykroczenia, czynności te [tu: czynności wyjaśniające] w

Wskazać należy, iż realizacja przez straż gminną zadań nałożonych na nią ustawowo wymaga wykorzystywania informacji o osobach, których działania te dotyczą. Przepisy ustawy o strażach gminnych wprost stanowią o prawie straży gminnej do przetwarzania danych w związku z realizacją określonych prawem zadań, bez konieczności uzyskania na to zgody osoby, której dane dotyczą. Oznacza to, iż straż gminna, na mocy stosownych przepisów rangi ustawowej, ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie niezbędnych jej danych osobowych, zaś operator ten winien – mając na względzie fakt realizacji obowiązku czuwania przez straż gminną nad przestrzeganiem prawa przez obywateli – udostępnić informacje w zakresie wnioskowanym przez straż (i adekwatnym do potrzeb prowadzonego przez straż postępowania). W takiej sytuacji dochodzi bowiem do realizacji dyspozycji z przepisu art. 161 ust. 1 in fine ustawy Prawo telekomunikacyjne. Generalny Inspektor zauważył, iż problem ten jest związany z interpretacją wynikających z ww. przepisów norm prawnych, co jednakże może oznaczać, iż nie dopełniają one zasad techniki prawodawczej. Zdaniem organu do spraw ochrony danych osobowych ustawa powinna wyczerpująco regulować daną dziedzinę spraw, nie pozostawiając poza zakresem swego unormowania istotnych fragmentów tej dziedziny, zaś przepis prawa materialnego powinien możliwie bezpośrednio i wyraźnie wskazywać kto, w jakich okolicznościach i jak powinien się zachować, natomiast wyjątkowo wskazywać tylko zachowanie nakazywane albo zakazywane jego adresatowi, jeżeli adresat lub okoliczności tego nakazu albo zakazu są wskazane w sposób niewątpliwy w innej ustawie.[238] Pożądane zmiany przepisów ustawy o strażach gminnych powinny uwzględnić potrzebę przetwarzania przez straże gminne ograniczonego katalogu danych objętych tajemnicą telekomunikacyjną. Katalog ten mógłby obejmować dane identyfikujące użytkownika sieci telekomunikacyjnej w zakresie jego imienia i nazwiska, adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania, ewentualnie nazwy firmy i siedziby prowadzenia działalności[239].

Generalny Inspektor Ochrony Danych Osobowych wskazał jednocześnie, iż prawo do ochrony danych osobowych nie może pozostawać w oderwaniu od innych przepisów prawa, i

---

miarę możności należy podjąć w miejscu popełnienia czynu bezpośrednio po jego ujawnieniu i zakończyć w ciągu miesiąca.

[238] § 3 i 25 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. Nr 100, poz. 908)

[239] Problem ten dotyczy w szczególności braku unormowań przepisów ustawy o strażach gminnych podobnych do postanowień art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. 2015 r. poz. 355 z późn. zm.), czy art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. 2014 r. poz. 1402 z późn. zm.), które to przepisy określają zasady i tryb udostępniania danych.

czynników, które należy mieć na względzie bez zakładania a priori, iż prawo do ochrony danych osobowych, będzie zawsze prawem nadrzędnym.[240] Dodatkowo w doktrynie podkreśla się, iż „(...) wytyczając reguły ochrony danych osobowych, należy uważać, aby nie przekroczyć granicy, za którą trafne i szlachetne zamiary oraz założenia zaczynają już wywoływać negatywne skutki. Ma to miejsce na przykład wówczas, gdy zbyt rygorystyczne ograniczenia w pozyskiwaniu i gromadzeniu informacji (danych osobowych) przeszkadzają w należytym zapewnieniu porządku i bezpieczeństwa"[241].

Pismem z dnia 7 września 2015 r. Minister Spraw Wewnętrznych odnosząc się do wystąpienia, nie podzielił stanowiska GIODO wskazując, iż nadanie straży gminnej uprawnień do dostępu do danych objętych tajemnicą telekomunikacyjną w sprawach o wykroczenia spowoduje, że formacja ta posiadałaby uprawnienia do pozyskiwania danych objętych tajemnicą telekomunikacyjną, w zakresie szerszym, niż posiada Policja, czy Straż Graniczna.

14) wystąpienie w związku z zamieszczeniem w Biuletynie Informacji Publicznej niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy, zawierających dane osobowe pracowników kontrolowanego urzędu

Pismem z dnia 18 maja 2015 r.[242] Generalny Inspektor Ochrony Danych Osobowych wystosował na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych wystąpienie do urzędu miejskiego w związku z zamieszczeniem w Biuletynie Informacji Publicznej niezanonimizowanego protokołu kontroli przeprowadzonej przez inspektorów pracy, zawierającego dane osobowe pracowników kontrolowanego urzędu. W tym samym przedmiocie organ ds. ochrony danych wystąpił do urzędu skarbowego. Generalny Inspektor Ochrony Danych Osobowych wskazał, iż taka praktyka nie jest zgodna z przepisami prawa.

[240] Stosownie do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 12 maja 2008 r. (sygn. II SA/Wa 229/2008), w którym WSA orzekł, iż cyt.: „Z art. 1 ust. 2 ustawy o ochronie danych osobowych wynika, iż przysługujące każdemu prawo do ochrony dotyczących go danych osobowych nie ma charakteru absolutnego, bowiem przetwarzanie danych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą lub dobro osób trzecich w zakresie i trybie określonym ustawą". Natomiast zgodnie z art. 1 ust. 1 ustawy o ochronie danych osobowych, każdy ma prawo do ochrony dotyczących go danych osobowych. W myśl zaś art. 1 ust 2 ustawy, 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. Oznacza to, iż w przypadku zaistnienia uzasadnionej okoliczności (przesłanki legalności), racjonalny ustawodawca dopuszcza przetwarzanie danych osobowych, także objętych tajemnicą prawnie chronioną, w celu innym, niż zostały zebrane. Przetwarzaniem danych osobowych – w myśl art. 7 pkt 2 ustawy o ochronie danych osobowych – jest m.in. ich zbieranie.

[241] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona Danych Osobowych Komentarz, 4 wydanie, Kraków 2007, str. 303-304

[242] DOLiS-035-4294/13

Organ do spraw ochrony danych osobowych w ww. wystąpieniach wskazał, iż udostępnieniu podlega informacja publiczna o danych publicznych, w tym treść i postać dokumentów urzędowych, w szczególności: treści aktów administracyjnych i innych rozstrzygnięć; dokumentacja przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających[243]. W orzecznictwie przyjmuje się, że informacją publiczną będzie każda wiadomość wytworzona przez szeroko rozumiane władze publiczne oraz osoby pełniące funkcje publiczne, a także inne podmioty, które w zakresie swoich kompetencji realizują władzę publiczną, bądź gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Informację publiczną stanowi więc treść dokumentów urzędowych czy wystąpień i ocen dokonywanych przez organy władzy publicznej, niezależnie do jakiego podmiotu są one kierowane i jakiej sprawy dotyczą[244]. W wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 2005 r. w sprawie II SAB/Wa 44/05 wskazano, że jak stanowi art. 6 ust. 1 pkt 4 lit. a) tiret drugie ustawy o dostępie do informacji publicznej, protokół i notatka z kontroli przeprowadzonej przez Państwową Inspekcję Pracy są informacją publiczną.

Organ do spraw ochrony danych jednocześnie przypomniał, że prawo do dostępu do informacji publicznej nie jest nieograniczone[245]. Ograniczenie 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. W związku z powyższym, przed ewentualnym opublikowaniem kopii protokołu z kontroli, dokument powinien zostać poddany zabiegowi anonimizacji w odniesieniu do danych osobowych pracowników. Nieuzasadnione udostępnienie przez pracodawcę informacji o pracowniku można rozpatrywać w kontekście naruszenia jego prawa do prywatności, w którym zawiera się prawo do ochrony danych osobowych i niewątpliwie pracodawca powinien powstrzymać się od działań, które będą naruszały zarówno dobra osobiste jak i prywatność pracownika.

[243] W myśl art. 8 ust. 3 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2015 poz. 2058, z późn. zm.) podmioty, o których mowa w art. 4 ust. 1 i 2, a więc m.in. podmioty reprezentujące jednostki organizacyjne samorządu terytorialnego obowiązane są do udostępniania w publikatorze teleinformatycznym tj. Biuletynie Informacji Publicznej (BIP) informacji publicznych, o których mowa w art. 6 ust. 1 pkt 1-3, pkt 4 lit. a) tiret drugie, lit. c) i d) i pkt 5, w tym dokumentacji przebiegu i efektów przeprowadzanych kontroli, jak również mogą udostępniać w BIP inne informacje publiczne.

[244] Wyroki NSA z dnia 30 października 2002 r. II SA 181/2002 i II SA 1956/2002

[245] Zgodnie z art. 5 ust. 2 ustawy o dostępie do informacji publicznej, prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy

Na administratorze danych osobowych spoczywają konkretne obowiązki określone w ustawie o ochronie danych osobowych. Z punktu widzenia niniejszej sprawy istotny jest obowiązek ustanowiony w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, zgodnie z którym administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Wyrażona w tym przepisie zasada adekwatności oznacza, że „swym rodzajem i swą treścią dane nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania”[246].

Ponadto administrator danych jest zobowiązany do wypełnienia obowiązku określonego w art. 36 ust. 1 ustawy o ochronie danych osobowych to jest zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. W szczególności administrator powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W ocenie Generalnego Inspektora w sprawie przy publikacji protokołu kontroli Państwowej Inspekcji Pracy oraz wystąpień pokontrolnych nie uwzględniono prawa do prywatności. Szczególne zastrzeżenia przy publikacji protokołów PIP budzi ujawnianie danych osobowych pracowników wskazanych urzędów (nazwisk pracowników wraz z informacjami na temat ich zdrowia w związku z wypadkami, jakim ulegli).

Podkreślenia wymaga fakt, że dla udostępnienia danych osobowych niezbędne jest istnienie ku temu odpowiedniej podstawy prawnej, zaś ustawa o dostępie do informacji publicznej jest podstawą do udostępnienia jedynie informacji publicznej. Ponadto w każdym przypadku konieczne jest uwzględnienie ograniczeń w prawie do informacji publicznej wynikających m.in. z ochrony prywatności osoby fizycznej zapisanych w art. 5 niniejszej ustawy.

Mając powyższe na uwadze, Generalny Inspektor Danych Osobowych zwrócił się do urzędu miejskiego oraz urzędu skarbowego o podjęcie działań mających na celu zaprzestanie publikowania danych osobowych osób fizycznych w treści protokołów oraz podjęcie działań mających na celu wyeliminowanie podobnych nieprawidłowości w przyszłości.

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

W odpowiedzi na wystąpienia Generalnego Inspektora Ochrony Danych burmistrz miasta poinformował, iż protokoły kontroli przeprowadzonej przez inspektorów pracy zawierające dane pracowników kontrolowanych urzędów zostały zanonimizowane i w takiej wersji zamieszczone w Biuletynie Informacji Publicznej. Wskazał również, iż w celu wyeliminowania podobnych nieprawidłowości w przyszłości, podjęto decyzję o zorganizowaniu szkolenia dla pracowników urzędu w tym zakresie.

15) kolejna grupa wystąpień dotyczyła powszechnej nieprawidłowości, polegającej na nieukrywaniu w masowej wysyłce korespondencji elektronicznej adresów e-mailowych adresatów[247]

Na wstępie przypomniano administratorom danych, 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 identyfikacji z wykorzystaniem dodatkowych informacji będących w posiadaniu administratora danych lub innych osób[248].

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 adresów e-mailowych innych odbiorców komunikatu - nie posiadają ku temu przesłanki legalności przetwarzania danych, o której mowa w art. 23 ust.1 ustawy.

[247] Np. DOLiS-035-1157/15; DOLiS-035-4294/13; DOLiS-035-3225/14; DOLiS-035-538/15.

[248] Zgodnie 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 dana 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.

Dlatego też za dobra 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.

16) wystąpienie w związku z podjęciem przez GIODO informacji, iż podczas przeprowadzania czynności urzędowych przez pracowników urzędu gminy dochodzi do przetwarzania danych osobowych w sposób umożliwiający zapoznanie się z nimi osobom do tego nieuprawnionym

Generalny Inspektor Ochrony Danych Osobowych pismem z dnia 21 sierpnia 2015 r. wystąpił do urzędu gminy w związku z powzięciem informacji, iż podczas przeprowadzania czynności urzędowych przez pracowników urzędu dochodzi do przetwarzania danych osobowych w sposób umożliwiający zapoznanie się z nimi osobom do tego nieuprawnionym. W konsekwencji, osobie, której dane dotyczą - w obecności osób trzecich - zadawane były pytania mające związek z obowiązkiem meldunkowym. Mając powyższe na uwadze Generalny Inspektor wskazał, że stosowanie takiego rozwiązania budzi wątpliwości pod kątem jego zgodności z powszechnie obowiązującymi przepisami prawa, w tym w szczególności przepisami ustawy o ochronie danych osobowych.

Na wstępie organ do spraw ochrony danych podkreślił że istotą ochrony danych osobowych jest ochrona prywatności osoby, której dane dotyczą. Źródło tej ochrony wynika przede wszystkim z przepisów Konstytucji RP.

Dyspozycję art. 51 ust. 5 Konstytucji RP wypełnia ustawa o ochronie danych osobowych, która określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach

danych (art. 2 ust. 1 ustawy). Na gruncie ustawy, o zgodnym z prawem przetwarzaniu[249] danych osobowych, mówić można jedynie w sytuacji, gdy ich administrator dopełnia wszelkich określonych jej przepisami obowiązków. Zgodnie 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[250]. Nadrzędnym obowiązkiem administratora danych osobowych[251], zgodnie z art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych jest dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w tym poprzez przetwarzanie danych osobowych zgodnie z prawem (zasada legalizmu). Ta generalna zasada znajduje swoje rozwinięcie w przepisach ustawy o ochronie danych osobowych określających m.in. wymogi, jakie powinien spełniać administrator danych w celu zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Jednym z podstawowych obowiązków spoczywających na administratorze jest, wynikający z art. 36 ust. 1 ustawy o ochronie danych osobowych, 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.

Generalny Inspektor Ochrony Danych Osobowych, powołując się na art. 36 ust. 2 przypomniał o obowiązku prowadzenia przez administratora dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych[252].Administrator danych – zgodnie z art. 38 ustawy – jest

[249] Art. 7 pkt 2 – przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych.

[250] 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. 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.

[251] Zgodnie z definicją zamieszczoną w art. 7 pkt 4 ustawy o ochronie danych osobowych jest 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.

[252] Dokumentacja taka powinna określać m.in. wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe. Podkreślenia wymaga również, iż zgodnie z art. 37

obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Osoby, które zostały upoważnione do przetwarzania danych, są zaś obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 ust. 2 ustawy).

Organ do spraw ochrony danych podkreślił, iż podstawą zachowania danych osobowych w tajemnicy jest z całą pewnością ujawnianie ich jedynie podmiotom, które do pozyskiwania przedmiotowych danych wykazują odpowiednią podstawę prawną. Wykonywanie obowiązków służbowych przez pracownika urzędu państwowego musi pozostawać w zgodzie z obowiązującym na terenie Rzeczypospolitej Polskiej stanie prawnym, w tym z ustawą o ochronie danych osobowych.

Wskazać należy, iż wszelkie czynności związane z przetwarzaniem danych osobowych winny być wykonywane z uwzględnieniem wszelkich środków technicznych i organizacyjnych zapewniających ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym. Z powyższego wynika zatem, że ich odpowiedniego zastosowania wymaga nie tylko proces przetwarzania danych osobowych w systemach informatycznych, czy w zbiorach tradycyjnych, ale także każda inna wykonywana na nich operacja, zatem i proces przechowywania dokumentów zawierających dane osobowe. Istotnym jest bowiem wdrożenie takich rozwiązań w przedmiocie zabezpieczania danych i kontroli tego procesu, który do minimum ograniczy możliwość wystąpienia nieprawidłowości w zakresie przetwarzania danych osobowych oraz przeszkolenie i wyczulenie na tę kwestię wykonujących te czynności pracowników.

Jednocześnie podkreślić należy, iż administrator musi mieć pełną kontrolę nad procesem przetwarzania danych, tak aby zapobiec powstawaniu zdarzeń narażających dane na udostępnienie osobom nieupoważnionym. Musi też mieć pełną wiedzę na temat całości procesu przetwarzania oraz weryfikować zachowanie pracowników pod kątem przestrzegania przez nich zasad ochrony danych osobowych, odpowiada bowiem także za ich działanie, co potwierdza nie tylko doktryna, ale i utrwalone orzecznictwo administracyjne[253].

W tym miejscu wskazać również trzeba, że administrujący danymi, który nie wypełni obowiązków przewidzianych cytowanymi powyżej przepisami, może ponosić odpowiedzialność karną na gruncie przepisów art. 51 ust. 1 oraz art. 52 ustawy o ochronie

---

ustawy o ochronie danych osobowych, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

[253] Por. wyrok Naczelnego Sądu Administracyjnego z dnia 4 kwietnia 2003 r., sygn. II SA 2935/02.

danych osobowych. Jak bowiem stanowią wspomniane przepisy, kto administrując zbiorem danych lub będąc obowiązanym do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2[254].

Mając powyższe na uwadze Generalny Inspektor Danych Osobowych zwrócił się do Wójta Gminy w Osieku o podjęcie stosownych działań mających na celu wyeliminowanie na przyszłość sytuacji, w których dochodzi do zapoznania się przez osoby nieuprawnione z danymi znajdującymi się w wyłącznej dyspozycji Urzędu Gminy w Osieku, co stanowi naruszenie przepisów ustawy o ochronie danych osobowych i prowadzić może do powstania odpowiedzialności administracyjnej, cywilnej jak i karnej. Do zapoznawania się z danymi osobowymi interesantów urzędu nie może dochodzić także przy współudziale osób trzecich w czynnościach urzędniczych, szczególnie osób nie posiadających stosownego upoważnienia do przetwarzania danych osobowych. Omawianie spraw urzędowych z osobami przebywającymi na terenie urzędu niewątpliwie stoi w sprzeczności z przepisami ustawy o ochronie danych osobowych.

17) wystąpienie w związku z uzyskaniem przez GIODO informacji, iż podczas kwalifikacji wojskowej dokonywanej przez komisję lekarską dane osobowe, w tym dane szczególnie chronione osób poddanych przedmiotowej kwalifikacji przetwarzane są w sposób umożliwiający zapoznanie się z nimi osobom do tego nieuprawnionym

Generalny Inspektor Danych Osobowych pismem z dnia 20 maja 2015 r.[255] wystąpił do wojewódzkiej komisji lekarskiej w związku z powzięciem informacji , iż podczas kwalifikacji wojskowej dokonywanej przez powiatową komisję lekarską nr 2 w Radomiu dane osobowe, w tym dane szczególnie chronione osób poddanych przedmiotowej kwalifikacji przetwarzane były w sposób umożliwiający zapoznanie się z nimi osobom do tego nieuprawnionym. Osobie, której dane szczególnie chronione dotyczą – w obecności osób trzecich – zadawane były pytania o stan zdrowia, takie jak historia przebytych chorób przewlekłych, czy też zażywania leków.

Generalny Inspektor wskazał, że stosowanie takiego rozwiązania budzi wątpliwości pod kątem jego zgodności z powszechnie obowiązującymi przepisami prawa, w tym w szczególności przepisami ustawy o ochronie danych osobowych oraz ustawy z dnia 6

[254] Odpowiedzialność ta rozszerzona została w art. 52 ustawy, zgodnie z którym penalizowane jest także nieumyślne naruszenie obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem.
[255] DOLiS-035-751/15

listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2016 r. poz. 186). Wskazać również należy, że obowiązek zachowania w tajemnicy związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu wynika również m.in. z przepisów ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2015 r. poz. 464 z późn. zm.), ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2014 r. poz. 1435 z późn. zm.), ustawy z dnia 20 lipca 1950 r. o zawodzie felczera (Dz. U. z 2012 r. poz. 1133 z późn. zm.). Również Kodeks Etyki Lekarskiej zobowiązuje do poszanowania intymności i prywatności pacjenta.

Ponadto pamiętać należy, że dane o stanie zdrowia to dane szczególnie chronione, których przetwarzanie, w myśl art. 27 ust. 1 ustawy o ochronie danych osobowych, jest co do zasady zabronione. Art. 27 ust. 2 pkt 7 wskazanej ustawy dopuszcza przetwarzanie danych szczególnie chronionych, w tym danych o stanie zdrowia, gdy jest to prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych. Jednakże powoływanie się na ten przepis uprawnione jest jedynie w odniesieniu do realizacji ściśle w tym przepisie wymienionych celów i nie może następować w celu uzasadniania udostępniania tych danych innym osobom. A zatem rozumiejąc konieczność administrowania rezerwami osobowymi dla celów powszechnego obowiązku obrony, wskazać należy, że osobom wobec których przeprowadzane jest określenie zdolności do służby wojskowej przysługuje prawo do ochrony tej sfery życia prywatnego, zwłaszcza gdy dotyczy to danych szczególnie chronionych, jakimi są dane o ich stanie zdrowia.

W omawianym przypadku nie sposób również przyjąć, iż spełnione są określone w art. 26 ust. 1 pkt 1-3 ustawy o ochronie danych osobowych zasady: legalizmu, celowości i adekwatności przetwarzania danych, jak też, iż zagwarantowane jest bezpieczeństwo danych (rozdział 5 ustawy o ochronie danych osobowych).

Przepis art. 26 ust. 1 ustawy wprowadza obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Realizacja obowiązku właściwego zabezpieczenia danych osobowych oznacza między innymi przyjęcie takiego sposobu przetwarzania danych, który wyeliminuje możliwość zapoznania się z danymi przez osoby do tego nieupoważnione (art. 36 ust. 1). Stosownie bowiem do art. 36 ust. 1 ustawy, każdy administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Szczególny reżim ochrony danych wrażliwych, w tym danych o stanie zdrowia) wyraża się ponadto w obowiązku zastosowania odpowiednich, uwzględniających charakter kategorii tych danych, środków oraz rozwiązań technicznych i organizacyjnych, które zapewnią tym danym, w konkretnych warunkach i okolicznościach przetwarzania, skuteczną i intensywną ochronę przed potencjalnymi zagrożeniami.

Niewywiązanie się z powyższych obowiązków może w konsekwencji prowadzić do powstania odpowiedzialności karnej na podstawie art. 51 i 52 ustawy. W myśl pierwszego ze wskazanych przepisów, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 51 ust. 2 ustawy). Zgodnie natomiast z art. 52 ustawy, kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Znamieniem przestępstwa określonego w art. 52 ustawy jest samo niedopełnienie obowiązku ochrony danych osobowych, choćby dane nie zostały zabrane, zniszczone lub uszkodzone.

Mając powyższe na uwadze Generalny Inspektor zwrócił się do wojewódzkiej komisji lekarskiej przy urzędzie wojewódzkim o podjęcie stosownych działań w tej sprawie.

9.3. 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),
- Infolinia (czynna od poniedziałku do piątku, w godzinach pracy Biura).

9.3.1. Współpraca ze środkami masowego przekazu

Stałe kontakty z mediami

Wzorem lat ubiegłych, w 2015 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 lokalnym i 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, Cyberlaw, lex.pl czy Panoptykon), 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 2015 r. Kontynuowana była również stała współpraca GIODO ze stacjami telewizyjnymi i radiowymi, m.in. z Informacyjną Agencją Radiową, Polskim Radiem Jedynką, Trójką Polskim Radiem, Czwórką Polskim Radiem oraz Polskim Radiem 24, Radiem TOK FM, Radiem dla Ciebie, TVP INFO, Telewizją Polsat, Superstacją czy TVN24. Zaowocowała ona emisją wielu programów o tematyce ochrony danych osobowych. Materiały i informacje

dotyczącej tej problematyki chętnie wykorzystywały również współpracujące z GIODO agencje informacyjne - PAP, KAI i Newseria.

W 2015 r. w prasie, radiu, telewizji i Internecie opublikowanych lub wyemitowanych zostało – zainicjowanych przez GIODO - ponad **70 materiałów prasowych o tematyce ochrony danych.** Przeważająca ich część jest dostępna na stronie internetowej GIODO (www.giodo.gov.pl).

1. 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 czy kamer montowanych w prywatnych samochodach,
- 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,
- przetwarzanie danych osobowych przez placówki opieki zdrowotnej, w tym m.in. wywoływanie pacjentów po nazwisku, umieszczanie tzw. kart gorączkowych przy łóżkach pacjentów, udostępnianie dokumentacji medycznej czy pozyskiwanie danych osobowych na potrzeby odbioru recept przez osoby trzecie,
- wyłudzanie danych osobowych w celach przestępczych, czego konsekwencją jest kradzież tożsamości,
- udostępnianie nieznanym podmiotom - przez osoby, których dane dotyczą - szczegółowych informacji na swój temat; sposoby wyłudzania danych i zagrożenia z tym związane,

- 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,
- 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,
- wprowadzanie przez gminy obowiązku oznaczania worków ze śmieciami nalepkami zawierającymi dane osobowe oraz adresy zamieszkania,
- przetwarzanie danych osobowych zarówno lekarzy, jak i pacjentów przez portale oceniające lekarzy,
- wprowadzenie przepisów zobowiązujących do zamieszczania numeru PESEL ucznia na legitymacji szkolnej,
- upublicznianie danych osobowych dłużników, np. na drzwiach wejściowych do budynków lub w Internecie.

W 2015 r. GIODO udzielił dziennikarzom ponad **400** odpowiedzi.

3. Wywiady i wystąpienia

Tematyka wywiadów radiowych i telewizyjnych czy wyjaśnień przekazanych prasie 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 w czasie pracy poprzez kontrole poczty e-mail, sprawdzanie bilingów 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, a także prawa osób, których dane dotyczą.

Wiele wywiadów udzielonych na początku 2015 r. dotyczyło - wchodzących w życie od 1 stycznia 2015 r. - zmian w ustawie o ochronie danych osobowych, w tym nowej roli i pozycji administratorów bezpieczeństwa informacji (ABI). 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 i prac legislacyjnych w Polsce, propozycja wprowadzenia systemu identyfikacji głosowej w biurach Krajowej Informacji Podatkowej, montowanie wideorejestratorów w prywatnych samochodach i udostępnianie nagrań nie tylko Policji, ale również umieszczanie ich w Internecie. Kolejnym wymagającym szerokiego omówienia przez GIODO problemem było zjawisko kradzieży tożsamości, które upowszechnia się coraz bardziej, przynosząc nie tylko finansowe, ale i wizerunkowe straty osobom, które zostały nim dotknięte. Sporo uwagi w przeprowadzonych z GIODO wywiadach dziennikarze poświęcili również wyciekom danych osobowych, bezpiecznemu korzystaniu ze zbliżeniowych kart płatniczych, a także dopuszczalności tworzenia przez przedsiębiorców profili osobowych klientów.

W 2015 r. GIODO udzielił ponad **90** wywiadów

4. Konferencje prasowe

W związku z potrzebą nagłośnienia niektórych wydarzeń lub upublicznienia stanowiska GIODO w istotnych dla ochrony danych osobowych sprawach, GIODO w 2015 r. zorganizował **8** konferencji prasowych. Poświęcone one były:

- obchodom IX Dnia Ochrony Danych Osobowych w Polsce i w Brukseli (28 stycznia 2015 r. w Warszawie, 20 stycznia 2015 r. w Brukseli),
- zamierzeniom GIODO na początku nowej kadencji (22 kwietnia 2015 r.),
- założeniom i konsekwencjom unijnej reformy prawa w zakresie ochrony danych osobowych. Omówiono najważniejsze z przepisów projektowanego unijnego rozporządzenia oraz wskazano na wpływ, jaki wywrze ono na działalność podmiotów przetwarzających dane osobowe. Przedstawiono też prawa, jakie przysługiwać będą każdej osobie, której dane dotyczą (14 maja 2015 r. w Łodzi),
- programowi edukacyjnemu GIODO „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”.

Podsumowane zostały efekty V edycji programu, dzięki któremu *ś*wiadomość w zakresie ochrony danych osobowych, zarówno u uczniów, ich rodziców, jak i nauczycieli jest coraz większa, tym bardziej że z roku na rok przystępuje do tej inicjatywy coraz więcej szkół. Wskazano też te obszary, na które trzeba zwracać szczególną uwagę w procesie edukacji. Zaliczono do nich m.in. konieczność edukowania w zakresie coraz powszechniejszego zjawiska hejtu i możliwości przeciwdziałanie mu wśród dzieci i młodzieży (28 maja 2015 r.),

- podsumowaniu pierwszego półrocza działania administratorów bezpieczeństwa informacji (ABI) po zmianie przepisów wzmacniających ich pozycję i rolę w powołujących ich instytucjach. Omówione zostały problemy praktyczne związane ze stosowaniem nowych przepisów dotyczących ABI (15 lipca 2015 r.),
- podsumowaniu prac nad unijnym rozporządzeniem o ochronie danych osobowych oraz dyrektywą dotyczącą przetwarzania danych osobowych w sektorze wymiaru sprawiedliwości. Omówiono najważniejsze założenia obu aktów prawnych oraz wskazano na konieczność odpowiedniego przygotowania się do ich wejścia w życie (18 września 2015 r.),
- ochronie danych osobowych w działalności służb specjalnych państwa, ze szczególnym uwzględnieniem projektowanych przepisów dostosowujących polskie prawo do orzeczeń sądów w sprawie retencji danych telekomunikacyjnych. Odniesiono się również do prac legislacyjnych nad unijną dyrektywą w sprawie ochrony danych przez właściwe organy policyjne i sądowe w sprawach karnych, a także do innych ważnych prac legislacyjnych w Unii Europejskiej, takich jak przyszłe ramy prawne funkcjonowania Europolu oraz Eurojustu, przetwarzanie danych osobowych pasażerów linii lotniczych (PNR) czy też projekty dotyczące inteligentnych granic (22 października 2015 r.),
- programowi edukacyjnemu GIODO „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". W związku z inauguracją VI jego edycji szczególną uwagę zwrócono na konsekwencje zachowań młodych ludzi w sieci. Wskazano, że systematyczne uświadamianie uczniów, jak powinni dbać o prywatność i dane osobowe zarówno innych, jak i własne, jak reagować w sytuacjach zagrożenia, to ważne zadanie szkół. Podkreślono, że GIODO wspiera je poprzez swój program edukacyjny, wokół którego buduje coraz większą koalicję (22 października 2015 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 2015 r. w Warszawie oraz 20 stycznia 2015 r. w Brukseli).

W ramach tych obchodów, wzorem lat ubiegłych, w siedzibie Redakcji „Dziennika Gazety Prawnej" odbył się panel dyskusyjny „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne" zorganizowany 27 stycznia 2015 r. przez GIODO oraz redakcję „Dziennika Gazety Prawnej". Zapis z debaty opublikowany został na łamach Gazety w dniu 3 lutego 2015 r.

Po raz kolejny tematy poruszane w czasie obchodów odbiły się dzięki mediom szerokim echem, co z pewnością przekłada się na lepszą edukację zarówno osób, których dane dotyczą, i tych, którzy dane przetwarzają.

b) Debaty i dyżury eksperckie

Nagłośnianiu istotnych z punktu widzenia ochrony danych osobowych zagadnień, służą również debaty organizowane w mediach od lat. W roku sprawozdawczym 2015 GIODO był współorganizatorem debaty w Redakcji Polityki InSight, która odbyła się 23 czerwca 2015 r. W czasie jej trwania poruszano takie tematy, jak projekt unijnego rozporządzenia w sprawie ochrony danych osobowych, sankcje za naruszenia przepisów dotyczących ochrony danych, a także funkcjonowanie Biura GIODO. W spotkaniu uczestniczyli abonenci Polityki Insight, do których należą m.in. dziennikarze i specjaliści z zakresu ochrony danych osobowych i prywatności.

GIODO brał też udział w 2 telefonicznych dyżurach eksperckich zorganizowanych przez Redakcję „Gazety Wyborczej", które odbyły się w warszawskiej siedzibie Redakcji 5 marca 2015 r. i 2 kwietnia 2015 r. Były one częścią organizowanej przez Gazetę akcji społecznej „Po stronie klienta", mającej na celu uwrażliwienie na kwestie wyłudzania czy kradzieży danych osobowych, by wykorzystać je w przestępczych celach. Efektem telefonicznego kontaktu z czytelnikami były publikacje udzielonych podczas dyżuru wyjaśnień i porad prawnych, które ukazały się na łamach „Gazety Wyborczej", jak i na jej stronie internetowej.

c) Wakacyjna kampania informacyjna

W 2015 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 udostępniony został poradnik poświęcony temu, jak chronić dane osobowe w różnych sytuacjach, w jakich znajdujemy się podczas wakacji. GIODO ostrzegał przed grożącymi nam negatywnymi konsekwencjami pozostawiania dowodu osobistego czy innych dokumentów potwierdzających tożsamość w zastaw za wypożyczony sprzęt. Uczulał też na niezgodną z prawem. publikację w Internecie zdjęcia, bez zgody przedstawionej na nim osoby. Radził, by przy upowszechnianiu wizerunku osób trzecich zachować szczególną rozwagę - nawet, gdy dotyczy to znajomych i bliskich nam osób. Wskazywał również, że przed zamieszczeniem zdjęcia dzieci, zawsze warto pomyśleć o konsekwencjach takiego działania w przyszłości. W poradniku „Co warto wiedzieć w czasie wakacji" znalazły się też inne istotne informacje będące przedmiotem kierowanych do Biura pytań, jak np. czy przewoźnik kolejowy ma prawo żądać od osoby kupującej bilet przez Internet podania numeru i serii dowodu osobistego, a także tego, czy konduktor w pociągu, który podejrzewa, że bilet i dokument potwierdzający tożsamość podróżnego są sfałszowane, może je zatrzymać.

Poradnik, zgodnie z zamysłem pomysłodawców wakacyjnej akcji, został zamieszczony na stronach internetowych blisko 40 urzędów i innych instytucji biorących w niej udział. Tematy poruszane w poradniku GIODO zostały również podjęte przez większość mediów - zarówno tradycyjnych, jak i elektronicznych.

6. Infolinia

Ważną rolę w działalności informacyjnej GIODO pełnił, czynny w godzinach pracy Biura od 8.00 do 16.00 telefon informacyjny – Infolinia. Utworzenie jej było odpowiedzią na ogromne zainteresowanie zagadnieniami dotyczącymi ochrony danych osobowych zarówno osób, których dane dotyczą, jak i podmiotów przetwarzających dane osobowe. Jednak ze względów organizacyjno-technicznych w lipcu 2015 r. działanie Infolinii zostało zawieszone. W 2015 r. za jej pośrednictwem udzielono wyjaśnień ponad **4 tysiącom** osób.

7. Newsletter

W 2015 r. GIODO kontynuował wydawanie Newslettera, dostarczanego wszystkim, wyrażającym chęć jego otrzymywania poprzez zarejestrowanie się za pośrednictwem strony internetowej GIODO. W 2015 r. przygotowane zostało **4** jego wydania.

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 o opiniach Grupy Roboczej Art. 29, której Generalny Inspektor członkiem.

9.3.2. Publikacje

1. **Broszura informacyjna w ramach V programu „Twoje dane – twoja sprawa. (…)"**

W ramach V ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli" przygotowana została przez Generalnego Inspektora Ochrony Danych Osobowych oraz Ministerstwo Administracji i Cyfryzacji, **broszura informacyjna dla nauczycieli pt. „Jak bezpiecznie zwiedzać cyfrowy świat"**. Przygotowany pakiet edukacyjno-informacyjny przedstawia zarys najważniejszych kwestii dotyczących tematyki ochrony danych osobowych i prywatności oraz bezpiecznego korzystania z Internetu przez dzieci. Wiedza na ten temat, ujęta w 7 podstawowych obszarów tematycznych, stanowi niezbędny element wychowania i edukacji szkolnej, zgodnie z podstawą programową wychowania przedszkolnego i kształcenia ogólnego w poszczególnych typach szkół.

2. **Publikacja „Enforcing privacy: lessons from current implementations for the future" w ramach projektu PHAEDRA**

Nakładem Wydawnictwa Sejmowego ukazała się książka pokonferencyjna „Egzekwowanie prywatności: wnioski z obecnego wdrażania i perspektywy na przyszłość". Publikacja zawiera szereg artykułów poświęconych problematyce praktycznej współpracy między organami ochrony danych, w tym także materiały zaprezentowane w trakcie konferencji podsumowującej realizację projektu PHADERA, która odbyła się w dniu 12 grudnia 2014 r. w Krakowie. Konferencja podsumowująca dwa lata realizacji projektu dała możliwość partnerom projektu, przedstawicielom środowiska organów ochrony danych

i prywatności oraz reprezentantom środowiska nauki i instytucji zajmujących się ww. problematyką do zaprezentowania aktualnego stanu wiedzy dotyczącej różnych aspektów współpracy i koordynacji między organami ochrony danych i prywatności. Wnioski z tych obserwacji, zebrane w publikacji pokonferencyjnej, stanowią doskonały materiał obrazujący aktualną sytuację w zakresie współpracy i koordynacji między organami ochrony danych i prywatności, a także dostarczają szeregu spostrzeżeń na temat możliwych przyszłych działań zmierzających do poprawy aktualnego stanu, prezentując także możliwe modele współpracy. Wszystkie te przemyślenia prowadzą do konkluzji, że efektywna współpraca między organami ochrony danych i prywatności jest zasadniczym elementem skutecznej ochrony podstawowego prawa do prywatności i ochrony danych osobowych[256].

9.3.3. Szkolenia podmiotów zewnętrznych

W ramach prowadzonej działalności edukacyjnej w 2015 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 2015 r. zwróciły się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o przeprowadzenie szkolenia znalazły się: Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Komenda Główna Policji, Warszawski Uniwersytet Medyczny, Prokuratura Okręgowa Warszawa Praga, Polski Instytut Dyplomacji im. Ignacego Jana Paderewskiego, Ministerstwo Spraw Zagranicznych, Krajowa Rada Spółdzielcza, Agencja Nieruchomości Rolnych, Prokuratoria Generalna Skarbu Państwa, a także Forum Sekretarzy Jednostek Samorządu Terytorialnego Województwa Lubelskiego, Polska Izba Przemysłu Targowego oraz sekretarze województwa warmińsko-mazurskiego.

Niektóre szkolenia miały cykliczny charakter, jak szkolenie realizowane w ramach VI edycji ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”.

W sumie w 2015 r. przeprowadzono **32 szkolenia** podmiotów zewnętrznych.

[256] Pełny tekst publikacji przygotowanej w języku angielskim dostępny jest na stronie internetowej projektu PHAEDRA http://www.phaedra-project.eu/?page_id=41.

9.3.4. Konkursy

W analizowanym 2015 r. Generalny Inspektor Ochrony Danych Osobowych był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

1. 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 V edycji konkursu było przygotowanie pracy na temat ujawniania danych osobowych studentów przez uczelnie innym podmiotom. Uczestnicy konkursu mieli za zadanie ustalić, czy uczelnia miała prawo – w przypadku podanym w kazusie – ujawnić dane osobowe studentów podmiotom, które zamierzały wyciągnąć wobec nich konsekwencje prawne za nielegalne ściąganie filmów w sieci i czy organ ds. ochrony danych osobowych może nakazać ujawnienie takich danych. 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.

2. Konkurs dla uczniów na infografiki – ochrona danych osobowych w pracach dzieci

Generalny Inspektor Ochrony Danych Osobowych 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 dla nauczycieli, zorganizowanymi przy współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów, który jest partnerem programu edukacyjnego Generalnego Inspektora. Celem warsztatów było przygotowanie nauczycieli do prowadzenia zajęć z uczniami w zakresie tworzenia infografiki

przy użyciu bezpłatnych aplikacji. Laureaci konkursu wraz z opiekunami wzięli udział w seminarium podsumowującym program edukacyjny w roku szkolnym 2014/2015, podczas którego wręczono nagrody.

3. Konkurs dla szkół i ośrodków doskonalenia nauczycieli

Już po raz trzeci 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 V edycji programu. W konkursie udział wzięło 16 szkół i 1 ośrodek doskonalenia nauczycieli. Główną nagrodę – Złote Pióro Programu otrzymało Gimnazjum Nr 132 z Oddziałami Integracyjnymi w Warszawie. Uroczystość wręczenia nagród odbyła się w dniu 28 maja 2015 r. podczas seminarium podsumowującego V edycję programu.

4. Konkurs na scenariusz lekcji nt. prawa do prywatności i ochrony danych osobowych

Generalny Inspektor Ochrony Danych Osobowych zaprosił nauczycieli szkół podstawowych, gimnazjów i szkół ponadgimnazjalnych, które realizowały VI edycję ogólnopolskiego programu edukacyjnego GIODO Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa skierowana do uczniów i nauczycieli", do opracowania scenariuszy lekcji w kontekście podstawy programowej kształcenia ogólnego, które wzbogacą tradycyjny program nauczania o elementy poszanowania prywatności i ochrony danych osobowych. Spośród zgłoszonych na konkurs 12 prac wybrany został jeden scenariusz zatytułowany „Kto chce Twoje dane osobowe?" opracowany przez nauczycieli Gimnazjum Nr 119 im. Marszałka Józefa Piłsudskiego w Warszawie. Jedną z nagród w tym konkursie była prezentacja zwycięskiego scenariusza podczas konferencji poświęconej edukacji dzieci i młodzieży, zorganizowanej przez GIODO w dniu 4 marca 2016 r. w Barcelonie oraz zamieszczenie ww. scenariusza w publikacji podsumowującej projekt ARCADES.

Konkurs organizowany był w ramach projektu ARCADES „Wprowadzenie kwestii związanych z ochroną danych oraz prywatnością do szkół w Unii Europejskiej"

finansowanego przez Unię Europejską w ramach programu Fundamental Rights and Citizenship.

9.3.5. Projekty i programy

W roku sprawozdawczym 2015, Biuro GIODO kontynuowało swój udział w różnego rodzaju projektach. Wśród nich wymienić należy projekt ARCADES, którego realizacja rozpoczęła się w 2014 r. i projekt PHAEDRA II. Programy te są finansowane ze środków Unii Europejskiej. Ponadto w 2015 r. kontynuowany był także krajowy program edukacyjny „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", który GIODO organizuje od 2009 r. pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.

1. Projekt PHAEDRA II

Biuro Generalnego Inspektora Ochrony Danych Osobowych rozpoczęło realizację projektu **PHAEDRA II** (Improving practical and helpful cooperation between data protection authorities II) finansowanego z środków Komisji Europejskiej w ramach programu Fundamental Rights and Citizenship "Action grants" (JUST/2013/FRAC/AG/6068) koordynowanego przez DG Justice (Dyrekcję Generalną Sprawiedliwości). Projekt ten stanowi kontynuację projektu PHAEDRA I realizowanego w latach 2013-2015 we współpracy z Vrije Universiteit Brussel (koordynator projektu), Trilateral Research & Consulting LLP z Wielkiej Brytanii (partner) oraz Universitat Jaume I z Hiszpanii (partner).

PHAEDRA to akronim wyrażenia „Improving Practical and Helpful cooperAtion bEtween Data PRotection Authorities" („Usprawnienie praktycznej i przydatnej współpracy miedzy organami ochrony danych").

Kontynuując prace podjęte w pierwszym projekcie, PHAEDRA II koncentruje się na identyfikacji, wypracowaniu oraz upowszechnianiu instrumentów umożliwiających **poprawę praktycznej współpracy między europejskimi organami ochrony danych osobowych**. Głównym obszarem zainteresowania będzie analiza czynników umożliwiających współpracę między tymi organami, szczególnie z uwzględnieniem reformy założeń ochrony danych osobowych zaproponowanych przez Komisję Europejską. Pomimo kontynuowania w 2015 r. prac nad przyjęciem nowej regulacji o ochronie danych, podstawą do prowadzenia analiz będą także dotychczasowe regulacje prawne obowiązujące w poszczególnych krajach członkowskich UE. W oparciu o te badania oszacowane zostaną możliwości stwarzane przez

obowiązujące i proponowane przepisy w kierunku wzmocnienia współpracy między organami ochrony danych osobowych oraz opracowane zostaną strategie zmierzające do lepszego wdrażania obecnego i nowego prawa w omawianym obszarze zagadnień. Ponadto biorąc pod uwagę fakt ciągłej pracy nad opracowaniem założeń nowej regulacji o ochronie danych, projekt PHAEDRA II dostarczy praktyczne instrumenty i mechanizmy poprawy współpracy między organami oraz wypracuje wytyczne w zakresie przepisów prawa. Projekt PHAEDRA II skoncentruje się na analizie **trzech głównych obszarów zagadnień** istotnych dla europejskich organów ochrony danych osobowych: zapewnienie spójności, wymiana różnych rodzajów informacji (włączając informacje niejawne) oraz koordynacja i współpraca w zakresie egzekwowania prawa. Czas trwania projektu wynosi 24 miesiące.

Pierwsze spotkanie partnerów w ramach projektu odbyło się 20 stycznia 2015 r. w Brukseli[257].

W ramach projektu PHAEDRA II zrealizowany został pierwszy etap badań polegający na zebraniu i przeanalizowaniu informacji pochodzących od europejskich organów ochrony danych osobowych, celem poznania opinii i poglądów na temat najlepszych sposobów poprawy praktycznej współpracy między nimi w kontekście reformy unijnych przepisów o ochronie danych osobowych oraz obecnie obowiązującego prawa. Informacje zebrane zostały w okresie kwiecień-maj 2015 roku w oparciu o wywiady lub ankiety przeprowadzone wśród 27 przedstawicieli europejskich organów ochrony danych osobowych oraz Europejskiego Inspektora Ochrony Danych. Zakres badań obejmował zagadnienia dotyczące wpływu ogólnego rozporządzenia o ochronie danych na działalność organów ochrony danych, w tym opinii na temat mechanizmu spójności czy one-stop shop, Europejskiej Rady Ochrony Danych oraz ich znaczenia dla współpracy pomiędzy europejskimi organami ochrony danych. Kolejnym aspektem przeprowadzonego badania była analiza wyzwań stojących przed organami ochrony danych w obszarze współpracy i koordynacji w kontekście nowych przepisów, zwłaszcza w zakresie egzekwowania prawa. Przedmiotem badania były też inne elementy objęte zakresem zainteresowania projektu PHAEDRA II (stworzenie repozytorium zawierającego kluczowe decyzje wydawane przez organy ochrony danych, analiza możliwości wspólnego rozpatrywania skarg przez kilka organów ochrony danych, identyfikacja uprawnień wykonawczych organów ochrony danych czy też obserwacja

[257] Szczegółowe informacje na temat projektu dostępne są na stronie internetowej http://www.phaedra-project.eu

rozwoju nowych technologii). W rezultacie opracowany został raport podsumowujący wyniki badań i prezentujący zasadnicze wnioski wynikające z przeprowadzonych analiz[258].

Podkreślenia wymaga, że nakładem Wydawnictwa Sejmowego ukazała się książka pokonferencyjna „Egzekwowanie prywatności: wnioski z obecnego wdrażania i perspektywy na przyszłość", która zawiera szereg artykułów poświęconych problematyce praktycznej współpracy między organami ochrony danych, w tym także materiały zaprezentowane w trakcie konferencji podsumowującej realizację projektu PHADERA (Kraków, 12.12.2015 r.). Wnioski z realizacji projektu, zebrane w publikacji pokonferencyjnej, stanowią doskonały materiał obrazujący aktualną sytuację w zakresie współpracy i koordynacji między organami ochrony danych i prywatności, a także dostarczają szeregu spostrzeżeń na temat możliwych działań zmierzających do poprawy aktualnego stanu, prezentując także możliwe modele współpracy. Wszystkie te przemyślenia prowadzą do konkluzji, że efektywna współpraca między organami ochrony danych i prywatności jest zasadniczym elementem skutecznej ochrony podstawowego prawa do prywatności i ochrony danych osobowych. Dokonane oceny i rekomendacje znajdujące się w publikacji są szczególnie istotne w kontekście reformy unijnych przepisów o ochronie danych osobowych, a zwłaszcza projektu rozporządzenia ogólnego o ochronie danych, które zobliguje europejskie organy ochrony danych osobowych do efektywnej współpracy, szczególnie w zakresie wdrażania prawa[259].

2. Projekt ARCADES

W 2015 r. kontynuowana była realizacja projektu ARCADES pn. „Wprowadzenie kwestii związanych z ochroną danych oraz prywatności do szkół w Unii Europejskiej" (Introducing d**A**ta p**R**ote**C**tion **A**n**D** privacy issu**E**s at school**S** 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.

[258] Raport dostępny jest na stronie internetowej projektu PHAEDRA http://www.phaedra-project.eu/?page_id=201

[259] Pełny tekst publikacji przygotowanej w języku angielskim dostępny jest na stronie internetowej projektu PHAEDRA http://www.phaedra-project.eu/?page_id=41.

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 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.

W 2015 r. w ramach projektu przygotowany został **Europejski poradnik. Nauczanie o ochronie danych i prywatności w szkołach.** Poradnik ma stanowić przydatne narzędzie dla tych szkół w UE, które chciałyby edukować dzieci i młodzież w zakresie ochrony prywatności i danych osobowych. Został napisany prostym i czytelnym językiem, tak aby pomóc nauczycielom znajdować właściwe słowa w dyskusji z dziećmi o ochronie danych osobowych i składa się z dziesięciu rozdziałów poruszających różne aspekty ochrony danych osobowych i prywatności, szczególnie istotne dla dzieci i młodzieży. Polska wersja Poradnika została zaprezentowana nauczycielom w Polsce podczas październikowego seminarium rozpoczynającego VI edycję Programu „Twoje dane-twoja sprawa", zaś angielska wersja dostępna jest na stronie projektu ARCADES[260].

Na zakończenie projektu przygotowana zostanie zaś 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.).

[260] http://arcades-project.eu/index.php/deliverables

3. Krajowy program edukacyjny

W 2015 r. kontynuowany był ogólnopolski program edukacyjny „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", adresowany 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.

Do programu mogą przystąpić szkoły podstawowe, gimnazja i szkoły ponadgimnazjalne oraz placówki doskonalenia nauczycieli. Uczestnicy programu korzystają 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.

W związku z realizacją programu w roku szkolnym 2014/2015 (V edycja), do którego przystąpiło 150 przedstawicieli szkół i placówek doskonalenia nauczycieli, Biuro GIODO wspólnie z Ministerstwem Administracji i Cyfryzacji opracowało broszurę dla nauczycieli pt. „Jak bezpiecznie zwiedzać cyfrowy świat". Przygotowany pakiet edukacyjno-informacyjny przedstawia zarys najważniejszych kwestii dotyczących tematyki ochrony danych osobowych i prywatności oraz bezpiecznego poruszania się w sieci. Wśród nich znalazły się następujące tematy: ochrona danych osobowych, prawo do prywatności w sieci, serwisy społecznościowe, cyfrowe ślady, komunikacja w sieci, działania niepożądane w sieci oraz gry i zabawy.

Natomiast inauguracja VI edycji programu w roku 2015/2016 tradycyjnie już rozpoczęła się od seminarium szkoleniowego zorganizowanego przez Generalnego Inspektora Ochrony Danych Osobowych w dniach 22-23 października 2015 r. 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 ww. pakiety edukacyjne 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, Komendy Głównej Policji, Fundacji Panoptykon oraz Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie. 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 przedmiotowym szkoleniu, zorganizowanym w ramach **projektu ARCADES** *„Wprowadzenie kwestii związanych z ochroną danych oraz prywatnością do szkół w Unii Europejskiej”* współfinansowanego przez Unię Europejską w ramach programu Fundamental Rights and Citizenship, udział wzięło 187 osób.

Podczas trwania VI edycji programu, Generalny Inspektor Ochrony Danych Osobowych zorganizował też konkurs na scenariusz lekcji, adresowany do nauczycieli szkół podstawowych, gimnazjalnych i ponadgimnazjalnych – uczestników tej edycji – którego nagrodą był m.in. udział i przedstawienie przedmiotowego scenariusza podczas konferencji zorganizowanej przez GIODO w Barcelonie.

9.3.6. Konferencje, seminaria, spotkania

W roku sprawozdawczym 2015, 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 czy Tydzień Zapobiegania Kradzieży Tożsamości, a także patronował wielu przedsięwzięciom, 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. IX Dzień Ochrony Danych Osobowych – 28 stycznia 2015 r.

W styczniu 2015 r. Generalny Inspektor Ochrony Danych Osobowych już po raz dziewiąty organizował obchody Dnia Ochrony Danych Osobowych ustanowionego 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 IX Dniem Ochrony Danych Osobowych odbywały się zarówno w Brukseli, jak i we wszystkich stolicach państw członkowskich Unii Europejskiej.

Uroczystości z okazji Dnia Ochrony Danych Osobowych organizowane są cyklicznie od 2007 r. Z tej okazji, jak co roku, Generalny Inspektor Ochrony Danych Osobowych zorganizował konferencję poświęconą najaktualniejszym zagadnieniom dotyczącym prawa do prywatności i ochrony danych osobowych, podczas której odbyła się też 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 „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne". Konferencja stanowiła kluczowy głos w dyskusji nad reformą ochrony danych osobowych, jak również była okazją do nabycia istotnych informacji i materiałów dotyczących nowelizacji przepisów ustawy o ochronie danych osobowych obowiązujących od 1 stycznia 2015 roku.

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 IX Dnia Ochrony Danych Osobowych, organizując wydarzenia podkreślające wagę ochrony prywatności i danych osobowych.

W dniu 29 stycznia 2015 r. w Warszawie, Biura GIODO przy współpracy z Urzędem m.st. Warszawa zorganizowało zajęcia dla dzieci „Moje dane, mój skarb" w ramach akcji „Zima w mieście". Podczas dwugodzinnych warsztatów przeprowadzonych przez przedstawicieli Biura GIODO, uczniowie z warszawskich szkół podstawowych mieli okazję dowiedzieć się, jak ważna jest ochrona danych osobowych i poszanowanie prawa do prywatności. Celem zajęć z uczniami (kl. 4-6) było podkreślenie, jak cenna jest nasza prywatność i jaka jest wartość naszych danych osobowych we współczesnym świecie. Zajęcia były również okazją do refleksji na temat tego, jak bezpiecznie korzystać z osiągnięć nowoczesnych technologii i świadomie unikać zagrożeń w Internecie.

Obchodom IX Dnia Ochrony Danych Osobowych towarzyszyły również wydarzenia za granicą. Z tej okazji w Brukseli zaplanowano okolicznościowe spotkanie z europejskimi rzecznikami ochrony danych.

2. IX Kongres Business Intelligence (Warszawa, 7.05.2015)

Omówieniu najciekawszych rozwiązań, narzędzi i metod zarządzania systemem analityki biznesowej poświęcony był IX Kongres Business Intelligence, który odbył się pod patronatem honorowym Generalnego Inspektora Ochrony Danych Osobowych. Podczas tego wydarzenia swoje prezentacje wygłosiła dr Edyta Bielak-Jomaa, GIODO, oraz jej zastępca – Andrzej Lewiński.

3. Seminarium podsumowujące V edycję programu edukacyjnego GIODO (Warszawa, 28 maja 2015 r.)

Seminarium poświęcone było zagadnieniom związanym z bezpieczeństwem młodzieży szkolnej oraz ich prawem do prywatności i ochrony danych osobowych. W jego trakcie odbyło się uroczyste wręczenie nagród laureatom konkursów zorganizowanych w ramach V edycji ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Uczestnikami seminarium podsumowującego program byli nauczyciele, dyrektorzy szkół i ośrodków doskonalenia nauczycieli, a także przedstawiciele sektora oświaty oraz eksperci w dziedzinie edukacji na rzecz bezpieczeństwa w szkołach.

4. Konferencja „Działalność służb specjalnych Państwa a ochrona danych osobowych" (Warszawa, 22.10.2015)

Funkcjonowanie służb specjalnych w Polsce w świetle przepisów o ochronie danych osobowych było głównym tematem konferencji zorganizowanej przez Generalnego Inspektora Ochrony Danych Osobowych i Centralne Biuro Antykorupcyjne, przy współpracy Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Wydarzenie to stanowiło ważny wkład w dyskusję dotyczącą praw i wolności obywateli oraz uprawnień służb specjalnych w kontekście nadchodzących zmian legislacyjnych w Polce i Unii Europejskiej, w szczególności orzecznictwa Trybunału Sprawiedliwości UE oraz wyroku Trybunału Konstytucyjnego RP w sprawie retencji danych.

5. III Międzynarodowa Konferencja i Wystawa „Cyber Security – bezpieczeństwo ponad granicami" (Warszawa, 26.11.2015)

Konferencja skupiła specjalistów, decydentów oraz praktyków w zakresie wykorzystania technologii informatycznych w celu wielowymiarowej ochrony gospodarczego, politycznego i militarnego bezpieczeństwa Państwa. Podczas sesji

„Bezpieczeństwo sieci teleinformatycznych w administracji i gospodarce" wystąpił przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych, który przedstawił prezentację poświęconą sposobom przeciwdziałania negatywnym zjawiskom w sieci i ograniczanie ich skutków. Organizatorem tego wydarzenia był Zarząd Targów Warszawskich S.A.

6. Spotkanie u Rzecznika Praw Obywatelskich (Warszawa, 15.12.2015)

Zmiany w ustawach dotyczących funkcjonowania rynku finansowego stały się bodźcem do zorganizowania spotkania instytucji Rzeczników, których zadaniem jest rozpatrywanie skarg dotyczących rynku usług finansowych oraz zapewnienie przestrzegania praw osób korzystających z tych usług. Celem tego spotkania, które z udziałem Generalnego Inspektora Ochrony Danych Osobowych odbyło się w siedzibie RPO w Warszawie, było ocena wpływu nowych regulacji na prawa jednostki oraz wypracowanie mechanizmu współpracy różnych instytucji dla możliwie najlepszego zapewnienia ochrony osób, będących odbiorcami dostępnych na rynku usług finansowych.

9.3.7. Porozumienia o współpracy

1. Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, 16.04.2015 r.

W dniu 16 kwietnia w Gdyni podpisane zostało porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a Wyższą Szkołą Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, reprezentowana przez J.M. Rektora prof. zw. dr hab. Jerzego Młynarczyka. Współpraca będzie realizowana 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, organizować seminaria, konferencje, szkolenia, praktyki studenckie oraz wspólnie podejmować prace naukowe i badawcze z zakresu ochrony danych osobowych

2. Instytut Nauk Prawnych Polskiej Akademii Nauk, Warszawa 22.06.2015 r.

Zawarte w dniu 22 czerwca 2015 r. porozumienie przewiduje współpracę GIODO z INP PAN w zakresie działalności naukowo-badawczej oraz edukacyjnej dotyczącej ochrony danych osobowych oraz prawa do prywatności. Porozumienie to jest pierwszą umową o

współpracy z instytutem naukowym i stanowi kontynuację działań GIODO wspierających edukację specjalistów z dziedziny ochrony danych osobowych. Jednym z pierwszych efektów współpracy jest objęcie przez GIODO patronatu nad powołanym przez Instytut Nauk Prawnych PAN studium podyplomowym „Wykonywanie funkcji administratora bezpieczeństwa informacji", którego celem jest kształcenie osób pełniących tę funkcję pod kątem zmienionych przepisów o ochronie danych osobowych oraz przyszłej regulacji prawnej Unii Europejskiej.

3. Komendant Główny Policji oraz Wyższa Szkoła Policji w Szczytnie, 17.09.2015 r.

W dniu 17 września 2015 r. w Warszawie podpisane zostało porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych a Komendantem Głównym Policji oraz Wyższą Szkołą Policji w Szczytnie. Współpraca obejmuje wspólne przedsięwzięcia w obszarze działalności naukowo-badawczej, edukacyjnej, szkoleniowej, promocyjnej, wydawniczej, organizacyjnej oraz w zakresie wykonywania obowiązków przez Administratora Bezpieczeństwa Informacji. Porozumienie jest efektem dotychczasowej wieloletniej współpracy Komendy Głównej Policji i Generalnego Inspektora Ochrony Danych Osobowych w zakresie właściwego stosowania przepisów ustawy o ochronie danych osobowych, w ramach której zorganizowano do tej pory szereg szkoleń prowadzonych przez przedstawicieli Biura GIODO, spotkań konsultacyjnych i konferencji.

Mając na uwadze, że w świetle nowych europejskich przepisów o ochronie danych osobowych, które wkrótce staną się powszechnie obowiązującym prawem we wszystkich państwach członkowskich Unii Europejskiej, konieczne jest podjęcie działań mających na celu właściwe ich dostosowanie do specyfiki zadań związanych z działalnością Policji, Generalny Inspektor Ochrony Danych Osobowych podjął decyzję aktywniejszego wsparcia działalności Policji, zgłaszając swój udział w przedsięwzięciach edukacyjnych Wyższej Szkoły Policji w Szczytnie, a także innych jednostek Policji. Zasadniczym celem porozumień jest wymiana doświadczeń w obszarach związanych z zapewnieniem skutecznej ochrony danych osobowych, zwiększenie wiedzy każdej osoby o jej prawach i środkach ochrony danych osobowych jak również podwyższenie poziomu wiedzy zawodowej i profesjonalnych umiejętności praktycznych funkcjonariuszy Policji i pracowników. W ramach współpracy przewiduje się m.in. prowadzenie monitoringu krajowych i światowych rozwiązań w zakresie ochrony danych osobowych, realizację projektów krajowych i unijnych w obszarze ochrony

danych osobowych i w systemach utrzymania bezpieczeństwa i porządku publicznego, podejmowanie działań edukacyjnych skierowanych do dzieci i młodzieży oraz przedsięwzięć na rzecz bezpieczeństwa danych osobowych w cyberprzestrzeni i w Internecie, a także wspólną organizację seminariów, konferencji, szkoleń i warsztatów oraz realizację prac naukowych i badawczych z zakresu ochrony danych osobowych.

4. Wydział Prawa i Administracji Uniwersytetu Warszawskiego. Warszawa, 5.11.2015 r.

Działalność naukowo-badawcza, edukacyjna, a także dotycząca promocji i wydawnictw, to przewidywane obszary wspólnej aktywności obu stron porozumienia. Będzie ona dotyczyła m.in. takich zagadnień, jak: prowadzenie monitoringu krajowych i światowych rozwiązań ochrony prywatności, danych osobowych oraz tajemnic prawnie chronionych, współorganizowanie seminariów, sympozjów i konferencji naukowych. W ramach współpracy edukacyjnej i dydaktycznej będą prowadzone szkolenia z udziałem zarówno ekspertów z GIODO, jak i z UW. Planuje się również wspólną realizację projektów zewnętrznych (krajowych i unijnych) w obszarze ochrony prywatności, danych osobowych i tajemnic prawnie chronionych,. W obszarze zaś działalności wydawniczej przewidziane jest wspólne wydawanie monografii i materiałów konferencyjnych dotyczących ochrony prywatności i danych osobowych. Dodatkową wartością tej umowy jest zapowiedź utworzenia – przy merytorycznym i kadrowym wsparciu GIODO – studiów podyplomowych na Wydziale Prawa i Administracji UW. Porozumienie zostało zawarte 5 listopada 2015 r. Podpisała je dr Edyta Bielak-Jomaa, Generalny Inspektor Ochrony Danych Osobowych (GIODO) oraz prof. dr hab. Krzysztof Rączka, Dziekan Wydziału Prawa i Administracji. Podczas uroczystości obecni byli także minister Andrzej Lewiński, zastępca GIODO oraz prof. dr hab. Tomasz Giaro, Prodziekan ds. współpracy z zagranicą i kadry naukowej.
To już kolejne, 16. porozumienie organu ds. ochrony danych osobowych z wyższą uczelnią.

10. 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).

10.1. 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 2015 r. kontynuowane były prace Komitetu T-PD z zakresu 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 32. posiedzenia plenarnego T-PD, które odbyło się w dniach 1-3 lipca 2015 r., członkowie Komitetu przeanalizowali projekt

sprawozdania wyjaśniającego do zmodernizowanej wersji Konwencji nr 108 oraz przyjęli **opinię dotyczącą Rekomendacji Zgromadzenia Parlamentarnego 2067 (2015) w sprawie „masowego nadzoru**". Opracowany także został Program prac Komitetu T-PD na lata 2016-2017, w którym przewidziano m.in. prace nad kwestią ochrony danych dotyczących pasażerów linii lotniczych (PNR) oraz prace nad rewizją rekomendacji w sprawie ochrony danych medycznych. Podkreślenia wymaga, że wymienione kwestie były tematem 36. i 37. posiedzenia Biura T-PD, które odbyły się kolejno w Paryżu (6-8.10.2015 r.) i w Strasburgu (9-11.12.2015 r.).

10.2. Grupa Robocza Art. 29

W omawianym roku sprawozdawczym 2015, 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[261] 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[262].

W analizowanym roku 2015, Grupa Robocza Art. 29 opracowała następujące dokumenty:

1. Kompleksowa analiza wyników kontroli w zakresie plików cookie – sprawozdanie (WP 229);

[261] Art. 30 ust. 1 dyrektywy 95/46/WE.
[262] Art. 15 ust. 3 dyrektywy 2002/58/WE.

2. Oświadczenie GR Art. 29 w sprawie automatycznej międzypaństwowej wymiany danych osobowych w celach podatkowych (WP 230);
3. Dokument wyjaśniający w sprawie wiążących reguł korporacyjnych przetwarzającego (WP 204);
4. Opinia 1/2015 w sprawie kwestii ochrony danych i prywatności dotyczących wykorzystania dronów (WP 231);
5. Opinia 2/2015 w sprawie kodeksu postępowania dotyczącego przetwarzania danych w chmurze opracowanego przez grupę roboczą C-SIG (Cloud Select Industry Group) (WP 232);
6. Aktualizacja opinii 8/2010 w sprawie prawa właściwego w świetle wyroku TSUE w sprawie Google Spain (WP 179)
7. Wytyczne dla państw członkowskich dotyczące kryteriów zapewnienia zgodności z wymogami ochrony danych w kontekście automatycznej wymiany danych osobowych do celów podatkowych (WP 234);
8. Opinia 3/2015 dotycząca Dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych (WP 233).

10.3. 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 2015 roku Agencja Praw Podstawowych rozpoczęła prace nad projektem „Dane biometryczne w wielkoskalowych systemach IT UE w obszarze granic, wiz i azylu –

implikacje dla praw podstawowych". W pierwszej fazie APP poprzez swoich partnerów z FRANET przeprowadziła studium identyfikujące potencjalne problemy w poszczególnych państwach członkowskich. Do drugiej fazy projektu wybrano 6 państw członkowskich - wśród nich Polskę - w których w 2016 r. zostaną przeprowadzone wywiady m.in. z administratorami danych, organami ochrony danych, organami, które mają dostęp do poszczególnych systemów, a także z prawnikami i organizacjami świadczącymi pomoc prawną cudzoziemcom. Wywiady mają być także prowadzone z funkcjonariuszami na granicach, jak i z pracownikami konsulatów państw członkowskich w państwach trzecich. Wywiady będą prowadzone także z osobami, których dane dotyczą tj. aplikantów wizowych, osób składających wnioski o azyl, osoby zatrzymane w związku z nielegalnym przekraczaniem granic lub z nielegalnym pobytem na terytorium państw członkowskich oraz składające skargi w związku z przetwarzaniem ich danych w SIS, VIS lub Eurodac. Planowane jest przeprowadzenie ok. 300 wywiadów w każdym państwie członkowskim i po 50 wywiadów w placówkach dyplomatycznych w państwach trzecich. Analizę przeprowadzonych wywiadów i raport końcowy APP planuje przedstawić dopiero w 2017 r. W dniu 25 września 2015 r. odbyło się spotkanie, którego miało na celu omówienie projektu kwestionariusza, będącego podstawą wywiadów. W spotkaniu wzięli udział przedstawiciele: organów ochrony danych, organów ścigania, EDPS, KE, FRONTEX, organizacji pozarządowych i uczelni wyższych. Uczestnicy zostali podzieleni na grupy robocze zgodnie ze swoimi kompetencjami. Przedstawiciel GIODO brał udział w grupie roboczej, które zajęła się częścią kwestionariusza poświęconą prawu do informacji i prawu do dostępu, poprawienia lub usunięcia danych. Inne grupy zajęły się m.in. profilowaniem, pobieraniem odcisków palców i wykorzystywaniem środków przymusu, dostępem do baz danych i przekazywaniem danych do państw trzecich. Na koniec przeprowadzono sesję wspólną, gdzie omówiono wszystkie zmiany wprowadzone przez różne podgrupy robocze. Co do zasady pytania zaproponowane przez APP powinny zostać przeformułowane i doprecyzowane, tak aby była łatwo zrozumiałe dla respondentów. Dodatkowo wskazano, że ze względu na różnice techniczne pomiędzy poszczególnymi systemami część pytań powinna wyraźnie wskazywać do którego z systemów się odnosi. Większość uczestników wyraziła także niezadowolenie, że pomimo trwającego kryzysu migracyjnego projekt nie został zmodyfikowany i nie zostały do niego dołączone kraje, które w tej chwili rejestrują najwięcej wniosków azylowych, a także wskazywano na bardzo odległy termin zakończenia projektu, co *de facto* może oznaczać, że raport APP będzie się odnosił do nieistniejącej już sytuacji

faktycznej i prawnej. Jednakże APP podkreśliła, że jest związana terminami wskazanymi w już wcześniej rozpisanych przetargach na przeprowadzenie wywiadów, więc założenia ogólne projektu nie mogą już ulec zmianie.

10.4. Inne

W ramach współpracy na forum międzynarodowym, Generalny Inspektor Ochrony Danych Osobowych w 2015 r. przekazywał regularnie swoje szczegółowe stanowiska do instrukcji na posiedzenia gremiów przygotowawczych Rady Unii Europejskiej, w odniesieniu do następujących **projektów aktów prawnych Unii Europejskiej**:

1. projektu rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), w ramach Grupy Roboczej Rady UE ds. wymiany informacji i ochrony danych osobowych (Working Party on Information Exchange and Data Protection - DAPIX), Komitetu Stałych Przedstawicieli Rządów Państw Członkowskich przy Unii Europejskiej (COREPER II) i Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (Rada WSiSW);
2. projektu dyrektywy w sprawie ochrony danych osobowych przetwarzanych do celów zapobiegania i zwalczania przestępczości, wykrywania i ścigania ich sprawców albo wykonywania orzeczeń sądowych w sprawach karnych, w ramach Grupy Roboczej Rady UE ds. wymiany informacji i ochrony danych osobowych (Working Party on Information Exchange and Data Protection - DAPIX), Komitetu Stałych Przedstawicieli Rządów Państw Członkowskich przy Unii Europejskiej (COREPER II) i Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (Rada WSiSW);
3. projektu rozporządzenia w sprawie Agencji Unii Europejskiej ds. Współpracy i Szkolenia w Dziedzinie Egzekwowania Prawa (Europol) w ramach prac Grupy Roboczej ds. egzekwowania prawa (Law Enforcement Working Party - LEWP), Komitetu Koordynacyjnego ds. współpracy policyjnej i sądowej w sprawach karnych (Coordinating Committee in the area of police and judicial cooperation in criminal matters - CATS), Komitetu Stałych Przedstawicieli Rządów Państw Członkowskich przy Unii Europejskiej (COREPER II) i Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych (Rada WSiSW).

Przedstawiciele GIODO brali także udział w następujących spotkaniach organów ochrony danych osobowych państw UE:

1. Grupa koordynująca nadzór nad Systemem Informacji Schengen drugiej generacji - SIS II (SIS II Supervision Coordination Group) – grupa w 2015 r. przyjęła przewodnik korzystania z prawa dostępu dla osób, których dane są przetwarzane w SIS II, a także przyjęty został model audyty bezpieczeństwa systemów SIS II, VIS i Eurodac. Grupa pracowała też nad wspólną metodologią inspekcji wpisów w SIS II;
2. Grupa koordynująca nadzór nad Wizowym Systemem Informacyjnym - VIS (VIS Supervision Coordination Group) - grupa w 2015 r. skupiła się przede wszystkim na kwestii dostępu do danych przetwarzanych w VIS przez uprawnione organy oraz na realizacji praw osób, których dane są przetwarzane w systemie;
3. Grupa koordynująca nadzór nad systemem Eurodac (Eurodac Supervision Coordination Group) - grupa w 2015 r. skupiła się przede wszystkim na sposobie wdrożenia nowego rozporządzenia w sprawie Eurodac;
4. Wspólny organ nadzorczy Europolu (Joint Supervisory Body of Europol) – organ skupił się przede wszystkim na projekcie nowego rozporządzenia o Europolu, kwestionariuszu w sprawie działania Krajowych Jednostek o Europolu oraz opracowania raportu dot. ofiar handlu ludźmi;
5. Wspólny organ nadzorczy ds. celnych (Joint Supervisory Authority Customs);
6. Grupa koordynująca nadzór nad Systemem Informacji Celnej - CIS (CIS Supervision Coordination Group).

W tym miejscu podkreślenia wymaga, że w dniu 11 grudnia 2015 r., podczas posiedzenia Grupy Koordynującej Nadzór Nad Systemem Informacji Celnej (CIS), w trakcie którego przyjęto poradnik praw osób, których dane są przetwarzane w CIS oraz wydłużono obowiązywanie dotychczasowego programu prac Grupy na rok 2016 r., zastępca dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej Biura GIODO, który dotąd pełnił funkcję wiceprzewodniczącego Grupy, został wybrany na jej przewodniczącego.

Grupa Koordynująca Nadzór nad Systemem Informacji Celnej (CIS) jest forum umożliwiającym koordynację działań dotyczących nadzoru nad Systemem Informacji Celnej pomiędzy Europejskim Inspektorem Ochrony Danych i krajowych organów ochrony danych osobowych na podstawie art. 37 rozporządzenia Rady (WE) NR 515/97 z dnia 13 marca

1997 r. w sprawie wzajemnej pomocy między organami administracyjnymi Państw Członkowskich i współpracy między Państwami Członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego.

10.5. 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 2015 roku, współorganizowanym przez GIODO, były uroczystości związane z obchodami **IX Europejskiego Dnia Ochrony Danych Osobowych, które tradycyjnie już odbywały się w Brukseli w styczniu 2015 r.** W trakcie obchodów tego święta Generalny Inspektor Ochrony Danych Osobowych zorganizował w dniu **20 stycznia 2015 r.** 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, a także dziennikarzy, którzy na co dzień angażują się w tematy związane z ochroną danych osobowych i prawa do prywatności.

Wśród innych ważnych wydarzeń o charakterze międzynarodowym, które odbyły się w 2015 r. z udziałem GIODO lub jego przedstawicieli znalazły się:

1. Konferencja o dronach (Budapeszt 5-6.02.2016 r.)

O ile drony same w sobie nie stanowią zagrożenia dla prywatności, to problem ten pojawia się w odniesieniu do ich wyposażenia, które wraz z oprogramowaniem, jak kamery, mikrofony, GPS-y, facial recognition, itp. mogą naruszać prywatność osób fizycznych, a także inne prawa, jak prawo do zgromadzeń, prawo do niedyskryminacji czy godności osobistej jednostki. Wykorzystywane do produkcji dronów nowoczesne technologie mogą ingerować bardzo głęboko w prywatność obywateli, ponieważ drony są stosunkowo małych rozmiarów i ciche w działaniu i przez to właściwe niewidoczne, a dodatkowo są łatwo dostępne ze względu na stosunkowo niskie ceny kupna. Uczestnicy konferencji wskazywali również na inne zagrożenia wynikające z faktu, że operatorzy i producenci dronów nie mają świadomości, że urządzenia te mogą przetwarzać dane osobowe, w związku z tym nie wprowadzają odpowiednich rozwiązań technicznych związanych z przetwarzaniem i

przechowywaniem danych, np. tych związanych z szyfrowaniem danych, czy wprowadzaniem odpowiedniej rozdzielczości zdjęć, tak aby przy ich robieniu uniknąć automatycznej identyfikacji osób trzecich znajdujących się na danym terenie.

W konferencji wzięli udział przedstawiciele krajowych organów ochrony danych osobowych Komisji Europejskiej, Europolu, przedstawiciele administracji węgierskiej (zarówno organy ścigania jak i urząd lotnictwa), naukowcy (głównie z węgierskich uczelni) oraz przedstawiciele organizacji badawczych (np. Trilateral).

2. Konferencja Edukacyjna nt. wyzwań dla prywatności (Skopje, 22-23.06.2015 r.)

W dniach 22-23 czerwca 2015 r., z okazji dziesięciolecia macedońskiego organu ochrony danych osobowych odbyła się w Skopje konferencja poświęcona wyzwaniom dla prywatności. Przedstawiciel GIODO został zaproszony przez organizatorów do wygłoszenia prezentacji dot. nowych możliwości współpracy organów ochrony danych osobowych w przyszłym rozporządzeniu ogólnym o ochronie danych osobowych w UE. W dniu 22 czerwca 2015 r. odbyła się cześć zamknięta konferencji poświęcona wprowadzaniu w państwach bałkańskich innowacyjnych rozwiązań opartych na danych. Wzięli w niej udział tylko przedstawiciele organów ochrony danych osobowych z regionu oraz zaproszeni goście z unijnych organów. Tą część konferencji sponsorował Google. Jego przedstawiciel wraz z ministrem ds. społeczeństwa informacyjnego moderowali dyskusję. Podczas tego wydarzenia przedstawiono tzw. Biała księgę, w której zebrano najbardziej innowacyjne rozwiązania wprowadzone w poszczególnych państwach regionu. Co do zasady dokument ten nie zawiera żadnych odniesień do ochrony danych osobowych, a jedynie odnosi się do wszelkich możliwości ponownego wykorzystywania danych publicznie dostępnych. W dniu 23 czerwca 2015 r. odbyła się cześć otwarta konferencji przeznaczona dla przedstawicieli organów ochrony danych z regionu, a także nauczycieli i przedstawicieli organizacji pozarządowych. Odbyły się trzy panele tematyczne dotyczące: reformy przepisów o ochronie danych osobowych w UE i Radzie Europy, współpracy regionalnej pomiędzy bałkańskimi organami ochrony danych osobowych oraz dotyczący inicjatyw edukacyjnych, mających na celu propagowanie bezpiecznego korzystania z Internetu i zwalczania nienawiści w Internecie. W trakcie konferencji strona macedońska promowała także swój program edukacyjny skierowany do szkół średnich, w który są zaangażowane wszystkie szkoły średnie w Macedonii, a przedstawiciele organu ochrony danych w każdej z tych szkół prowadzą zajęcia z nauczycielami, uczniami i rodzicami.

3. 37. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności (Amsterdam, 26-29.10.2015 r.)

W dniach 26-29 października 2015 r. w Amsterdamie odbywała się 37. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności, której gospodarzem jest holenderski organ ochrony danych. Międzynarodowe Konferencje to najważniejsze, poświęcone zagadnieniom ochrony danych osobowych i prywatności - odbywające się cyklicznie, od 37 lat - spotkania, w których biorą udział rzecznicy ochrony danych osobowych z Europy, na czele z Europejskim Inspektorem Ochrony Danych, jak i rzecznicy z całego świata, przedstawiciele instytucji UE, rządów państw, eksperci zajmujący się tą problematyką, przedstawiciele świata akademickiego, organizacje pozarządowe i międzynarodowe działające na rzecz praw człowieka, jak i przedstawiciele biznesu.
W dniach 26-27 października 2015 r. odbyła się sesja zamknięta, czyli coroczne spotkanie zrzeszające wyłącznie rzeczników ochrony danych i prywatności z całego świata. Jej istotnym punktem było przyjęcie następujących dokumentów: Rezolucji w sprawie sprawozdawczości zapewniającej przejrzystość, Rezolucji w sprawie ochrony prywatności i międzynarodowych działań humanitarnych, Rezolucji dotyczącej specjalnego sprawozdawcy ONZ ds. prawa do prywatności oraz Rezolucji w sprawie strategicznego kierunku Konferencji.

Natomiast w dniach 28-29 października 2015 r. odbywały się sesje otwarte 37. Międzynarodowej Konferencji. Tematem przewodnim obrad jest projekt „Privacy Bridges", w ramach którego dziewięciu uznanych ekspertów w dziedzinie ochrony prywatności z USA i UE opracowało 10 praktycznych propozycji mających na celu podniesienie poziomu ochrony danych osobowych w Unii Europejskiej i USA[263]. W ramach Międzynarodowej Konferencji odbył się także pierwszy warsztat zorganizowany w ramach projektu PHAEDRA II. Spotkanie, którego gospodarzem był Generalny Inspektor Ochrony Danych Osobowych, poświęcone było zagadnieniu współpracy europejskich organów ochrony danych w kontekście zasad jakie dla tej współpracy przewidziane są tekście ogólnego rozporządzenia o ochronie danych. W trakcie trzech sesji warsztatu dyskutowano m.in. na temat modelu współpracy oraz koordynacji działań organów ochrony danych osobowych w planowanych przepisach unijnych, praktycznym trudnościom, jakie napotykają w swojej międzynarodowej

[263] Sprawozdanie ekspertów dotyczące projektu dostępne jest na stronie: https://www.privacyconference2015.org/wp-content/uploads/2015/10/Privacy-Bridges-Paper-release-version.pdf

współpracy organy ochrony danych oraz planowanych działaniach i projektach usprawniających praktyczną współpracę miedzy rzecznikami ochrony danych i prywatności.

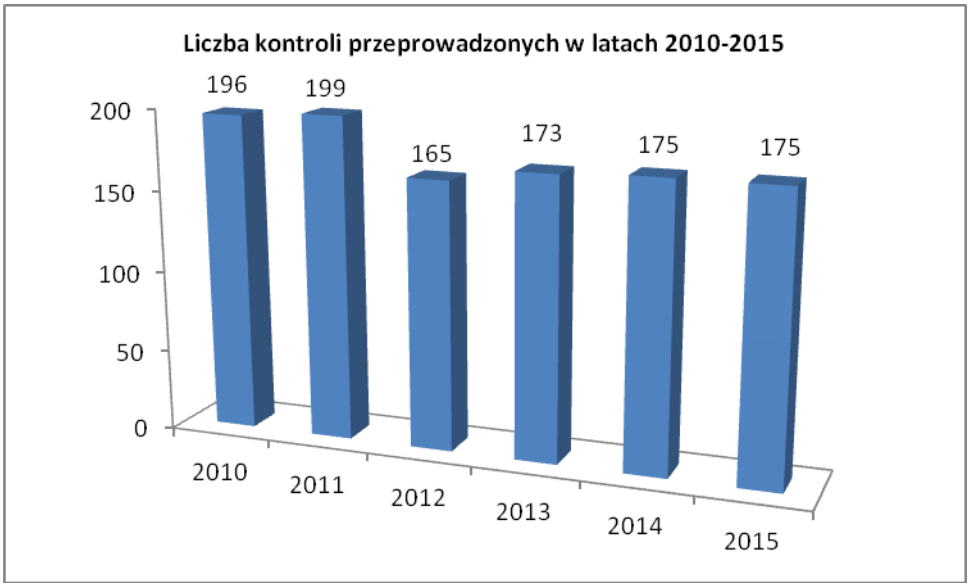
9.5. Wizyty robocze

1. Wizyta studyjna przedstawicieli chorwackiego organu ochrony danych osobowych

W dniach 4-6 maja 2014 r. w Biurze Generalnego Inspektora Danych Osobowych odbyła się wizyta studyjna przedstawicieli chorwackiego organu ochrony danych osobowych, współorganizowana przez Komisję Europejską w ramach mechanizmu TAIEX. Celem spotkania było pogłębienie wiedzy praktycznej o implementacji Systemu Informacyjnego Schengen (SIS), Wizowego Systemu Informacyjnego (VIS) i systemu Eurodac oraz wymiana dobrych praktyk dotyczących ochrony danych osobowych w tych systemach. W trakcie wizyty przedstawiciele Generalnego Inspektora Ochrony Danych Osobowych przedstawili podstawy prawne działania urzędu i zasady ochrony danych osobowych w Polsce, a także podstawy prawne działania SIS, VIS i Eurodac, ze szczególnym uwzględnieniem szczególnych uregulowań dotyczących ochrony danych osobowych. W spotkaniach uczestniczyli także przedstawiciele Komendy Głównej Policji, Komendy Głównej Straży Granicznej, Ministerstwa Spraw Zagranicznych, Urzędu do Spraw Cudzoziemców, którzy przedstawili swoją rolę w ww. systemach oraz przedstawiciele Helsińskiej Fundacji Praw Człowieka, którzy przedstawili sytuację cudzoziemców w Polsce i problemy związane z przetwarzaniem danych osobowych cudzoziemców w systemach krajowych i unijnych.

Część III. Charakterystyka działalności Generalnego Inspektora Ochrony Danych Osobowych w 2015 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 2015 r. przeprowadzonych zostało 175 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, tj. tyle samo co w analogicznym roku 2014.



Wykres 34: ***Porównanie liczby kontroli przeprowadzonych w latach 2010–2015.***

Czynnościom kontrolnym poddane zostały m.in. takie podmioty jak: operatorzy telekomunikacyjni, banki oraz administracja publiczna. Dużą grupę jednostek kontrolowanych stanowiły również podmioty zaliczone do sektora „Inne", 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 2015 r. wypożyczalnie sprzętu sportowego i audioprzewodników (12 kontroli), podmioty realizujące zadania wynikające z ustawy o Karcie Dużej Rodziny (12 kontroli), podmioty przechowujące dokumentację osobową i płacową (14 kontroli), podmioty lecznicze (7 kontroli) oraz organy przetwarzające dane w systemie Eurodac (3 kontrole). 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 **16 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 związku z nowelizacją ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn. zm.), na mocy której Generalny Inspektor

Ochrony Danych Osobowych z dniem 1 stycznia 2015 r. uzyskał uprawnienie zwracania się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46 c ustawy o ochronie danych osobowych, o **dokonanie sprawdzenia** określonego w art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych[264] u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia (art. 19b ust. 1 ustawy o ochronie danych osobowych[265]), w roku sprawozdawczym skierowano **13 wystąpień o dokonanie sprawdzeń przez administratorów bezpieczeństwa informacji** (zał. 3). Pierwsze wystąpienie o dokonanie sprawdzenia wystosowano do administratora bezpieczeństwa informacji powołanego przez Rzecznika Praw Obywatelskich (RPO)[266]. Przedmiotem sprawdzenia uczyniono przetwarzanie danych osobowych przez Rzecznika Praw Obywatelskich w zakresie monitoringu wizyjnego stosowanego w Biurze RPO. Na podstawie materiału dowodowego zebranego w oparciu o przesłane sprawozdanie oraz w wyniku prowadzenia korespondencji uzupełniającej, GIODO nie wniósł zastrzeżeń do sprawdzenia oraz stwierdził, że sprawozdanie zawierało wszystkie wymagane elementy, określone w art. 36c ustawy o ochronie danych osobowych. Dwanaście kolejnych wystąpień (tyle skierowano do ABI w czwartym kwartale 2015 r.) dotyczyło zabezpieczenia danych osobowych przez banki[267], w tym przez Narodowy Bank Polski[268]. W 2015 r. sprawozdania z tych sprawdzeń nie podlegały ocenie, gdyż pierwsze trzy wpłynęły do Biura GIODO z końcem grudnia 2015 r., a w stosunku do pozostałych nie upłynął termin do ich przedłożenia.

W analizowanym 2015 roku na ogólną liczbę 175 kontroli, 82 przeprowadzono w Warszawie (47%), zaś 93 poza Warszawą (53%).

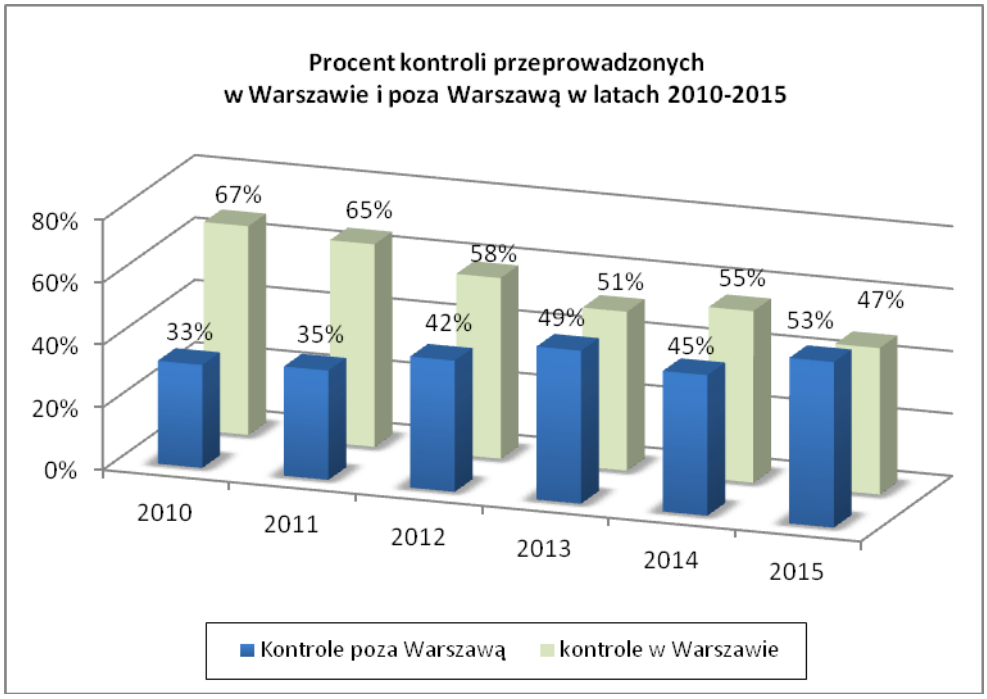
[264] Art. 36a.2.1.a). Do zadań administratora bezpieczeństwa informacji należy zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych.

[265] Art. 19b.1. Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia.

[266] Sygn. DIS-K-421/133/15/SPR1

[267] Np. sygn. DIS-K-421/161/15/SPR2, DIS-K-421/164/15/SPR3, DIS-K-421/208/15/SPR8, DIS-K-421/212/15/SPR12.

[268] Sygn. DIS-K-421/165/SPR4



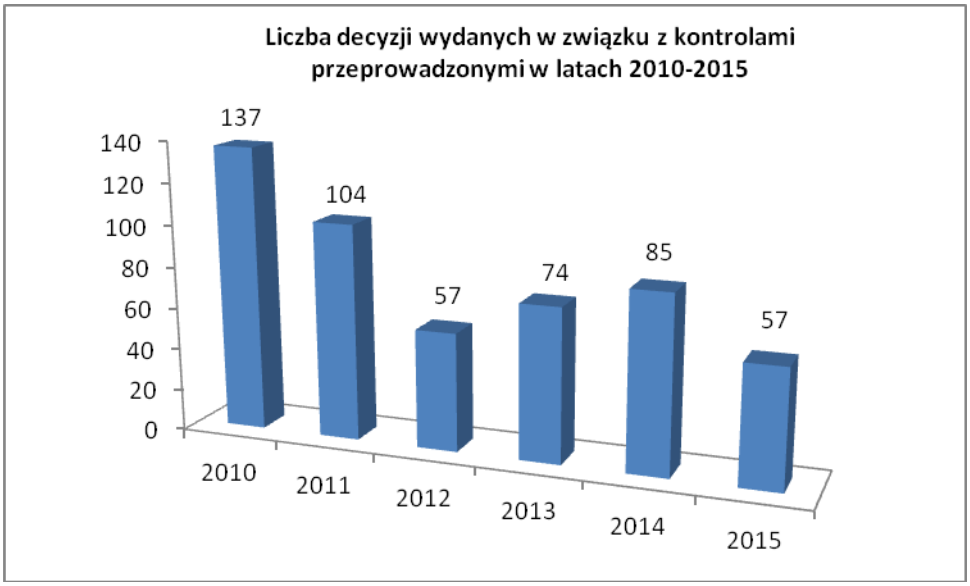
Wykres 35: ***Porównanie procentowe liczby kontroli przeprowadzonych w Warszawie i poza Warszawą w latach 2010–2015.***

Najwięcej kontroli przeprowadzonych zostało z urzędu (81). Poniższa tabela przedstawia liczbowe zestawienie kontroli ze względu na podmiot inicjujący.

Inicjatywa kontroli	Liczba kontroli
Departament Orzecznictwa, Legislacji i Skarg	52
Departament Rejestracji Zbiorów Danych Osobowych	16
Departament Edukacji Społecznej i Współpracy Międzynarodowej	2
Zespół ds. Egzekucji Administracyjnej	1
Prokuratura	3
Rzecznik Praw Obywatelskich	1
Urząd wojewódzki	1
W związku z inną kontrolą	5
Wystąpienia o dokonanie sprawdzenia	13
Inne	81
RAZEM	**175**

Do ogólnej liczby 162 kontroli przeprowadzonych w 2015 r. należy dodać wspomniane wcześniej 13 kontroli sprawdzających, wskutek skierowanych przez GIODO wystąpień do administratorów bezpieczeństwa informacji o dokonanie sprawdzenia.

W okresie sprawozdawczym w związku z przeprowadzonymi kontrolami wydanych zostało 57 decyzji administracyjnych oraz skierowano 4 zawiadomienia do organów ścigania o podejrzeniu popełnienia przestępstwa określonego w ustawie o ochronie o ochronie danych osobowych.



Wykres 36: ***Decyzje GIODO wydane w związku z kontrolami przeprowadzonymi w latach 2010 – 2015.***

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 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

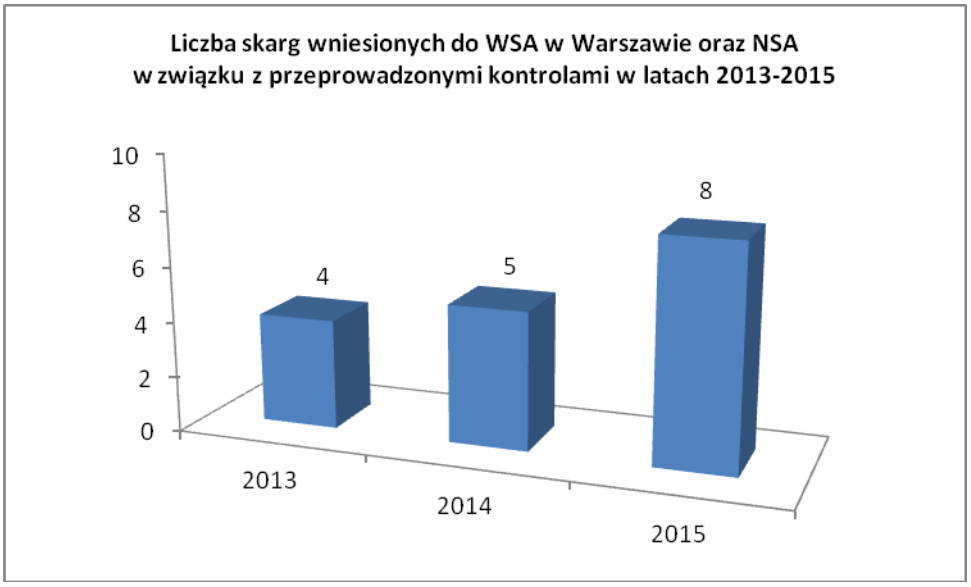
administratorzy danych, brak odpowiednich środków finansowych, niezbędnych do pokrycia kosztów związanych z wdrożeniem rozwiązań zapewniających prawidłowe spełnienie wymogów. W niektórych przypadkach przyczyny powyższego stanu rzeczy wynikały także z niewłaściwego podejścia osób odpowiedzialnych za przetwarzanie 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 2015 r. kontroli były podmioty, dla których ochrona przetwarzanych danych osobowych była ważnym zagadnieniem. Stosowane przez nie zasady przetwarzania danych osobowych odpowiadały wymogom wynikającym z przepisów o ochronie danych osobowych.

Na podkreślenie zasługuje fakt, że w wielu przypadkach działania inspektorów przeprowadzających kontrolę powodowały, że stwierdzone w trakcie kontroli uchybienia były usuwane przez jednostki kontrolowane w toku postępowania administracyjnego, a nawet jeszcze przed jego wszczęciem. Natomiast do nielicznych należały sytuacje składania przez te jednostki wniosków o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora oraz zaskarżania decyzji do Wojewódzkiego Sądu Administracyjnego w Warszawie. Podkreślić w tym miejscu także należy, że wydawane przez sądy administracyjne orzeczenia niejednokrotnie potwierdzały stanowisko Generalnego Inspektora Ochrony Danych Osobowych zaprezentowane w decyzjach administracyjnych wydanych na skutek przeprowadzonych kontroli.

Na podstawie ustaleń z kontroli przeprowadzonych w 2015 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 2015 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[269].

W związku ze złożonymi skargami na decyzje wydane na skutek przeprowadzonych kontroli, sądy administracyjne wydały osiem orzeczeń, w tym cztery orzeczenia wydał Wojewódzki Sąd Administracyjny w Warszawie i cztery Naczelny Sąd Administracyjny.



Wykres 37: ***Skargi wniesione do Wojewódzkiego Sądu Administracyjnego oraz Naczelnego Sądu Administracyjnego w związku z przeprowadzonymi kontrolami w latach 2013 – 2015.***

Do istotnych orzeczeń, jakie zapadły w okresie sprawozdawczym w sprawach, w których przeprowadzane były kontrole, należy wyrok z dnia 10 lipca 2015 r., sygn. akt II SA/Wa 2163/14, w którym Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę Prezydenta m.st. Warszawy. Wyrok ten był następstwem postępowania administracyjnego

[269] Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

prowadzonego przez Generalnego Inspektora po przeprowadzeniu w 2014 r. kontroli w Urzędzie Miasta Stołecznego Warszawy, w wyniku której stwierdzono nieprawidłowości w procesie przetwarzania danych osobowych na potrzeby realizowanego przez Prezydenta m.st. Warszawy projektu „Karta Warszawiaka" i „Karta Młodego Warszawiaka, w szczególności w zakresie braku podstaw prawnych do pozyskiwania danych osobowych 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. 1315 z późn. zm.).

W uzasadnieniu ww. wyroku Wojewódzki Sąd Administracyjny w Warszawie wskazał m.in., że Prezydent m.st. Warszawy jest upoważniony do wystąpienia o udostępnienie danych z CRP KEP, jednak wyłącznie, gdy działa jako organ podatkowy w związku z prowadzonym postępowaniem. Natomiast Prezydent m.st. Warszawy wykonując uchwały Rady Miasta Stołecznego Warszawy Nr LXVI/1807/2013 oraz nr LXVI/1806/2013 (w sprawie opłat za usługi przewozowe środkami lokalnego transportu zbiorowego w m.st. Warszawie), nie występuje w roli organu podatkowego w myśl przepisów ustawy z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. 2010 r. Nr 95 poz. 613 z późn. zm.). Zatem Prezydent m.st. Warszawy nie jest upoważniony do występowania na podstawie art. 15 ustawy o zasadach ewidencji i identyfikacji podatników i płatników, o udostępnienie danych z CRP KEP dla potrzeb realizacji projektu „Karta Warszawiaka" i „Karta Młodego Warszawiaka". Sąd wskazał również, że skoro z przepisów regulujących funkcjonowanie CRP KEP nie wynika możliwość wykorzystywania danych w nim zgromadzonych w celu weryfikowania uprawnień do zniżek lub ulg przewidzianych w ramach programu „Karta Warszawiaka" i „Karta Młodego Warszawiaka", prowadzonego przez Prezydenta m.st. Warszawy, Minister Finansów nie ma podstaw prawnych do przetwarzania danych osobowych zgromadzonych w rejestrze CRP KEP w ww. celu, w tym do ich udostępniania z przedmiotowego zbioru dla ww. celów. Ponadto Prezydent m.st. Warszawy nie jest uprawniony do pozyskiwania tych danych 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 danych uczestników programu „Karta Warszawiaka" lub „Karta Młodego Warszawiaka" w celu pozyskania informacji o tych osobach z CRP KEP. Wojewódzki Sąd Administracyjny podkreślił także, iż przekazywane przez Ministra Finansów informacje na temat zamieszkiwania (bądź nie) na terenie Warszawy przez osoby, których zapytanie dotyczy, dotyczą zidentyfikowanych osób. Nie budzi zatem żadnych wątpliwości w ocenie

sądu, że stosownie do treści art. 6 ust. 1 ustawy o ochronie danych osobowych, informacja na temat zamieszkiwania (bądź nie) na terenie Warszawy przez zidentyfikowaną osobę, stanowi dane osobowe w rozumieniu tej ustawy. W związku z powyższym sąd stwierdził, iż w ramach współpracy pomiędzy Prezydentem m.st. Warszawy a Ministrem Finansów miało miejsce udostępnianie danych osobowych z CRP KEP na potrzeby projektu „Karta Warszawiaka" i „Kartę Młodego Warszawiaka". Wojewódzki Sąd Administracyjny w Warszawie w uzasadnieniu przedmiotowego wyroku odniósł się również do umowy zawartej pomiędzy Prezydentem m.st. Warszawy a Ministrem Finansów. W ocenie sądu wskazana umowa nie miała charakteru umowy powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy o ochronie danych osobowych. Istotą instytucji powierzenia przetwarzania danych jest bowiem to, że wszystkie zlecone przez administratora danych operacje na danych powinny być wykonywane na rzecz administratora danych, na danych w tych celach przez niego powierzonych. W analizowanym przypadku dochodziło do udostępniania Ministrowi Finansów przez Prezydenta m.st. Warszawy, danych osobowych osób ubiegających się o „Kartę Warszawiaka" lub „Kartę Młodego Warszawiaka" w celu pozyskania informacji o osobach, których przekazane dane dotyczą, ze zbioru prowadzonego przez Ministra Finansów oraz do udostępniania przez Ministra Finansów z CRP KEP Prezydentowi m.st. Warszawy informacji na temat zamieszkiwania na terenie m.st. Warszawy przez osoby ubiegające się o hologram (poprzez wskazanie „tak" lub „nie") w celu weryfikacji uprawnień do otrzymania „Karty Warszawiaka" lub „Karty Młodego Warszawiaka". Celem przekazywania danych przez Prezydenta m.st. Warszawy Ministrowi Finansów nie było w istocie zlecenie Ministrowi Finansów wykonywania na rzecz Prezydenta m.st. Warszawy operacji na przekazanych danych osobowych, ale uzyskanie dodatkowych informacji o osobach, których przekazane dane dotyczą, ze zbioru prowadzonego przez Ministra Finansów, jako administratora danych. Ponadto Prezydent m.st. Warszawy również nie przetwarza pozyskanych od Ministra Finansów danych osobowych na rzecz Ministra Finansów, lecz wykorzystuje je do realizacji własnego celu, którym jest weryfikacja uprawnień do otrzymania „Karty Warszawiaka" lub „Karty Młodego Warszawiaka". Z powyższych względów zawarta pomiędzy Prezydentem m.st. Warszawy a Ministrem Finansów „umowa powierzenia przetwarzania danych osobowych" w sprawie współpracy w zakresie weryfikacji uprawnień osób zamierzających skorzystać z przyznanych zniżek lub ulg na zasadach określonych uchwałami Rady m.st. Warszawy, nie stanowi, wbrew jej nazwie, umowy powierzenia przetwarzania danych, o której mowa w art. 31 ustawy o ochronie danych

osobowych. W związku z powyższym, w ramach współpracy pomiędzy Prezydentem m.st. Warszawy a Ministrem Finansów dochodzi do wzajemnego udostępniania danych osobowych.

Podobnie wypowiedział się Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 15 lipca 2015 r., sygn. akt II SA/Wa 2280/14, oddalając skargę Ministra Finansów na decyzję Generalnego Inspektora utrzymującą w mocy decyzję nakazującą 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".

Do ciekawszych orzeczeń należał również wyrok z dnia 16 grudnia 2015 r., sygn. akt: II SA/Wa 658/15, Wojewódzkiego Sądu Administracyjnego w Warszawie, który oddalił skargę Spółki na decyzję Generalnego Inspektora z dnia 4 lutego 2015 r., sygn. DIS/DEC-71/15/8533, utrzymującą w mocy decyzję z dnia 6 listopada 2014 r., sygn. DIS/DEC-1072/14/87525. Wydając wskazane decyzje Generalny Inspektor nakazał podmiotowi prowadzącego klub fitness zaprzestanie przetwarzania bez podstawy prawnej danych biometrycznych klientów. Jak bowiem ustalono w toku kontroli, w wybranych klubach prowadzonych przez ten podmiot stosowany był system biometrycznej kontroli bezpieczeństwa. Wzorzec biometryczny odcisku palca klienta (informacje o pojedynczych punktach odcisku palca przekształcone algorytmem na postać cyfrową) zapisywany były w chipie opaski wydawanej klientowi. W celu wejścia do klubu, klient przykładał do czytnika znajdującego się przy bramce wejściowej opaskę i palec, w celu weryfikacji, czy jest on właścicielem opaski i ma uprawnienia do korzystania z oferty klubu. Czytnik odczytywał z opaski zapisany kod punktów biometrycznych i po przyłożeniu przez klienta palca do czytnika linii papilarnych odczytywał punkty biometryczne z palca, przetwarzał je w kod i porównywał z kodem zapisanym na opasce. W uzasadnieniu ww. wyroku Wojewódzki Sąd Administracyjny wskazał m.in., iż analiza stanu faktycznego nie pozwalała na przyjęcie tezy zaprezentowanej przez Spółkę, że przetwarzanie danych biometrycznych w czytniku, odbywało się poza systemem informatycznym oraz, że nie dochodzi w ten sposób do przetwarzania danych osobowych w postaci danych biometrycznych. Z tego powodu mianowicie, że na system informatyczny Spółki, o którym mowa w przepisie art. 7 pkt 2a

ustawy[270], składały się: system służący do obsługi klientów, system biometrycznej kontroli dostępu, urządzenia (w tym stacje komputerowe, urządzenia zapisujące dane biometryczne, czytniki danych biometrycznych, nośniki danych biometrycznych – opaski wydawane klientom spółki), a także opracowane i wdrożone procedury. Czytnik wraz z opaską są elementami tego systemu i służyły do identyfikacji klientów, którzy byli osobami zidentyfikowanymi poprzez przetwarzanie (przez Spółkę) m.in. imienia, nazwiska, nr PESEL, i to zarówno w postaci papierowej (umów członkowskich), jak i w systemie informatycznym służącym do obsługi klientów. Sąd wskazał, iż przetworzona do postaci cyfrowej dana biometryczna klienta, służyła do jego zidentyfikowania poprzez porównanie wzorca biometrycznego i pozwalała na dostęp do usług Spółki, a w konsekwencji spełniała przesłanki przepisu art. 6 ust. 1 ustawy. Jednocześnie Wojewódzki Sąd Administracyjny podzielił zdanie Generalnego Inspektora Ochrony Danych Osobowych, iż dana biometryczna była powiązana z danymi osobowymi klienta przetwarzanymi w systemie służącym do obsługi klienta poprzez numer ID i była pozyskiwana do zbioru danych osobowych klientów Spółki. Dane osobowe klientów przetwarzane przez Spółkę (m.in. w systemie służącym do obsługi klientów) wraz z ich danymi biometrycznymi tworzyły posiadający strukturę zestaw danych o charakterze osobowych, dostępnych według określonych kryteriów, a więc zbiór danych osobowych w rozumieniu art. 7 pkt 1 ustawy[271]. Zdaniem sądu nie można uznać tego zbioru za zbiór danych osobowych sporządzony doraźnie, wyłącznie ze względów technicznych, m.in. z uwagi na to, iż dane osobowe były przetwarzane w związku z zapewnieniem kontroli wstępu do klubów. Nie zmienia tego okoliczność relatywnie krótkiego okresu przetwarzania i wprowadzania tych danych do zbioru pojedynczo, tj. każdorazowo przy wejściu klienta Spółki do klubu w związku z przyłożeniem do czytnika palca i opaski. Ponadto Wojewódzki Sąd Administracyjnych wskazał, iż nie sposób uznać, aby Spółka przetwarzając dane osobowe biometryczne klientów legitymowała się podstawą prawną do ich przetwarzania, wskazaną w art. 23 ust. 1 pkt 1 i pkt 3 ustawy.

W innej sprawie Wojewódzki Sąd Administracyjny w Warszawie przychylił się do stanowiska Generalnego Inspektora Ochrony Danych Osobowych wyrażonego w decyzji skierowanej do podmiotu zajmującego się przewozem osób, w której nakazano usunięcie

[270] Art. 7 pkt 2a ustawy, ilekroć w ustawie jest mowa o systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

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

danych osobowych dotyczących numeru PESEL osób, które dokonały przez Internet rezerwacji w celu zakupu biletu na przejazd. W uzasadnieniu wyroku WSA podzielił stanowisko GIODO, iż w związku ze sprzedażą biletu przez Internet wystarczające było pozyskiwanie przez przewoźnika danych osobowych w następującym zakresie: imię, nazwisko, adres e-mail, numer telefonu komórkowego i hasło. WSA nie podzielił argumentów podmiotu kontrolowanego, iż przetwarzanie pozyskanych numerów PESEL dotyczących osób, które zakupiły bilet na przejazd przez Internet było potrzebne na wypadek ewentualnej kontroli skarbowej. WSA poparł argumentację Generalnego Inspektora, z której wynika, iż w trakcie całego postępowania podmiot kontrolowany nie podnosił tego argumentu, a po wszczęciu postępowania osoba zainteresowana zakupem biletu na przejazd, w celu założenia konta na stronie internetowej przewoźnika, nie wprowadza numeru PESEL, a jedynie takie dane jak: imię, nazwisko, adres e-mail, telefon komórkowy. W związku z tym dalsze przetwarzanie przez przewoźnika pozyskanych wcześniej numerów PESEL w celu prowadzenia rozliczeń finansowych, nie znajduje uzasadnienia. Jak wynikało z zebranego materiału dowodowego w niniejszej sprawie, przewoźnik dokonuje odpłatnego przewozu osób na podstawie umowy przewozu. Zawarcie wskazanej umowy następuje poprzez sprzedaż biletów dokonywaną przy użyciu kas fiskalnych lub za pośrednictwem systemu rezerwacji internetowej, tj. za pośrednictwem strony internetowej przewoźnika. Bilet zakupiony za pośrednictwem tej strony stanowi plik wygenerowany z systemu informatycznego, który zawiera następujące informacje: dane przewoźnika, imię i nazwisko podróżnego, datę i godzinę wyjazdu, cenę, liczbę oraz rodzaj zakupionych biletów a także specjalny unikatowy numer transakcji zakupu. Takie dane w dostateczny sposób potwierdzają transakcję zakupu biletu, o czym świadczy nadany w systemie informatycznym unikatowy numer tej transakcji, nadawany przez ww. system automatycznie po dokonaniu zapłaty za bilet. Tak więc przetwarzanie przez przewoźnika pozyskanych numerów PESEL, jako loginu, w celu prowadzenia rozliczeń finansowych nie znajduje uzasadnienia.

W związku z przeprowadzonymi **kontrolami** Generalny Inspektor skierował **w 2015 r. do organów ścigania 4 zawiadomienia o podejrzeniu popełnienia przestępstwa opisanego w ustawie o ochronie danych osobowych**. Jedno z zawiadomień było odpowiedzią na skargę skierowaną do Generalnego Inspektora, dotyczącą nieprawidłowości w procesie przetwarzania danych osobowych przez przedsiębiorcę zajmującego się świadczeniem usług telekomunikacyjnych. Z uwagi na fakt, iż przedsiębiorca nie odbierał korespondencji kierowanej do niego w tej sprawie, Generalny Inspektor podjął decyzję o przeprowadzeniu czynności kontrolnych w celu szczegółowego ustalenia stanu faktycznego w niniejszej

sprawie[272]. W celu zorganizowania przedmiotowej kontroli poinformowano pisemnie przedsiębiorcę o zaplanowanych czynnościach kontrolnych. W związku z brakiem odpowiedzi przedsiębiorcy na ww. pismo Generalny Inspektor wyznaczył nowy termin kontroli i jednocześnie poinformował przedsiębiorcę, że brak odpowiedzi na pismo w tej sprawie oraz uniemożliwienie przeprowadzenia kontroli inspektorom upoważnionym przez Generalnego Inspektora, może zostać potraktowane jako udaremnienie wykonania czynności kontrolnych i skutkować skierowaniem do prokuratury zawiadomienia o popełnieniu przestępstwa określonego w art. 54a ustawy o ochronie danych osobowych[273]. Podjęto również telefoniczną próbę kontaktu z przedsiębiorcą. Ustalono, że pod numerem telefonu znajdującym się na stronie internetowej zgłaszała się osoba nieupoważniona do reprezentowania przedsiębiorcy. Z uwagi na powyższe przekazano ww. osobie informację o kontroli i terminie jej przeprowadzenia wraz z prośbą o kontakt przedsiębiorcy z Biurem Generalnego Inspektora oraz z informacją o odpowiedzialności karnej w przypadku udaremnienia lub utrudniania inspektorowi wykonania czynności kontrolnej. Z Biurem Generalnego Inspektora skontaktował się telefonicznie pełnomocnik przedsiębiorcy, który poinformował, iż przedsiębiorca nie może brać udziału w czynnościach kontrolnych i z tego względu udzielił mu stosownego pełnomocnictwa do reprezentowania go w toku tych czynności.

W toku czynności kontrolnych przedsiębiorca jednak, za pośrednictwem pełnomocnika, przedstawił pisemne wyjaśnienia w zakresie przetwarzania danych osobowych skarżącego, które zostały załączone do akt kontroli, oraz przedłożył „pisemne zawiadomienie kontrolujących o sprzeciwie przedsiębiorcy wobec prowadzenia kontroli GIODO". Wobec powyższego czynności kontrolne u przedsiębiorcy zostały wstrzymane. Następnie do Biura Generalnego Inspektora wpłynął sprzeciw przedsiębiorcy wobec prowadzenia czynności kontrolnych, w którym nowy pełnomocnik przedsiębiorcy wskazał, iż żąda odstąpienia od kontynuowania kontroli w związku z rażącym naruszeniem przepisów prawa przez inspektorów Generalnego Inspektora. W odpowiedzi na ww. sprzeciw Generalny Inspektor wydał postanowienie o kontynuowaniu czynności kontrolnych[274], a także postanowienie o

[272] Kontrola DIS-K-421/125/15.
[273] Art. 54a. Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
[274] Postanowienie DIS/POST-443/15/87481.

utrzymaniu w mocy zaskarżonego postanowienia w związku ze złożonym przez przedsiębiorcę wnioskiem o ponowne rozpatrzenie sprawy[275].

W związku z powyższym, Generalny Inspektor skierował na adres pełnomocnika przedsiębiorcy pismo informujące o kontynuowaniu przez Generalnego Inspektora czynności kontrolnych. W piśmie poinformowano jednocześnie, że brak odpowiedzi na pismo oraz uniemożliwienie inspektorom przeprowadzenia kontroli może zostać potraktowane jako udaremnienie wykonania czynności kontrolnych i skutkować skierowaniem do prokuratury zawiadomienia o popełnieniu przestępstwa określonego w art. 54a ustawy o ochronie danych osobowych. Ww. pismo nie zostało odebrane przez pełnomocnika przedsiębiorcy, pomimo podwójnej jego awizacji. Zgodnie z art. 44 § 3 i 4 ustawy kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23) w przypadku niepodjęcia przesyłki w terminie, o którym mowa w § 2, pozostawia się powtórne zawiadomienie o możliwości odbioru przesyłki w terminie nie dłuższym niż czternaście dni od daty pierwszego zawiadomienia. Doręczenie uważa się za dokonane z upływem ostatniego dnia okresu, o którym mowa w § 1, a pismo pozostawia się w aktach sprawy.

Biorąc pod uwagę powyższe okoliczności Generalny Inspektor uznał, iż działania przedsiębiorcy stanowiły utrudnianie wykonania ustawowych uprawnień Generalnego Inspektora Ochrony Danych Osobowych, tj. przeprowadzenia czynności kontrolnych, co wyczerpuje znamiona czynu zabronionego, o którym mowa w art. 54a ustawy o ochronie danych osobowych. W konsekwencji, skierowane zostało do prokuratury zawiadomienie o popełnieniu przez przedsiębiorcę przestępstwa określonego w ww. przepisie ustawy o ochronie danych osobowych.

Analogiczna sytuacja miała miejsce w przypadku przedsiębiorcy prowadzącego portale internetowe. Przedsiębiorca ten uchylał się od przedstawienia wyjaśnień i dowodów w sprawie wniosku osoby, która złożyła skargę na nieudostępnienie danych osobowych (imienia, nazwiska, adresu zamieszkania, adresu e-mail oraz numeru IP) osób posługujących się określonymi loginami, zamieszczających wpisy na stronie internetowej prowadzonej przez przedsiębiorcę. Wpisy te, w ocenie skarżącego, zawierały nieprawdziwe i obraźliwe informacje na jego temat i tym samym naruszały jego dobra osobiste oraz podważały jego wiarygodność. Z uwagi na fakt, iż z przedsiębiorcą nie udało się nawiązać żadnego kontaktu, Generalny Inspektor podjął decyzję o przeprowadzeniu czynności kontrolnych w celu

[275] Postanowienie DIS/POST-475/15/94665.

szczegółowego ustalenia stanu faktycznego w sprawie. W celu przeprowadzenia kontroli próbowano ustalić w Internecie numer telefonu do tego podmiotu, lecz takiego numeru telefonu nie odnaleziono. Natomiast na stronie internetowej przedsiębiorcy podany był do kontaktu adres e –mail i w związku z tym, na ustalony adres została przesłana przez Generalnego Inspektora informacja o planowanym terminie kontroli. Z uwagi na okoliczność, iż przedsiębiorca nie skontaktował się z Biurem GIODO w terminie podanym w piśmie inspektorzy upoważnieni przez Generalnego Inspektora udali się pod adres głównego miejsca wykonywania działalności gospodarczej (adres wskazany w Centralnej Ewidencji i Informacji o Działalności Gospodarczej). Po przybyciu na miejsce ustalono, iż przedsiębiorca pod tym adresem już nie przebywa (lokal został sprzedany innej osobie). W związku z zaistniałą sytuacją inspektorzy GIODO podjęli kolejne czynności, w wyniku których ustalono, iż na stronie internetowej jednego z portali prowadzonego przez przedsiębiorcę podany był adres do obsługi korespondencji listowej tego portalu. Pomimo prawidłowego poinformowania przedsiębiorcy o kolejnym terminie kontroli, kontrola nie została przeprowadzona, gdyż pod tym adresem również nie zastano przedsiębiorcy. W następnym dniu po nieudanej próbie przeprowadzenia czynności kontrolnych do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła wiadomość e-mail, z której wynikało, iż przedsiębiorca skontaktuje się z Biurem GIODO w terminie późniejszym. Pomimo tej informacji nikt w tej sprawie nie skontaktował się z Biurem Generalnego Inspektora.

Biorąc pod uwagę przedstawione okoliczności, Generalny Inspektor uznał, iż powyższe działania przedsiębiorcy stanowią udaremnienie wykonania ustawowych uprawnień Generalnego Inspektora Ochrony Danych Osobowych, tj. przeprowadzenia czynności kontrolnych, co wyczerpuje znamiona czynu zabronionego, o którym mowa w art. 54a ustawy o ochronie danych osobowych. Z uwagi na powyższe, zawiadomiona została prokuratura o popełnieniu przez przedsiębiorcę przestępstwa określonego w powołanym przepisie ustawy o ochronie danych osobowych, polegającego na udaremnieniu wykonania czynności kontrolnych. Do Biura GIODO wpłynęło pismo z Policji informujące o wszczęciu dochodzenia w ww. sprawie.

Natomiast odnosząc się do charakterystyki **pytań prawnych**, wskazać należy, iż w omawianym okresie sprawozdawczym do Biura Generalnego Inspektora wpłynęło prawie **4 tysiące pism zawierających pytania z zakresu ochrony danych osobowych.**

Większość podmiotów kierujących pytania do Generalnego Inspektora Ochrony Danych Osobowych nadal stanowiły osoby fizyczne, w tym prowadzące działalność gospodarczą. 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. Zauważyć także trzeba, że wciąż duża jest liczba zapytań nadsyłanych przez podmioty zawodowo zajmujące się udzielaniem porad prawnych, jak i administratorów bezpieczeństwa informacji, czyli osoby, które powinny dysponować odpowiednią wiedzą z zakresu ochrony danych osobowych. 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 karnego, cywilnego, telekomunikacyjnego, dostępu do informacji publicznej, czy kompetencji innych organów publicznych.

Podkreślenia wymaga, że z natury rzeczy więc duża cześć z tych pytań 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.

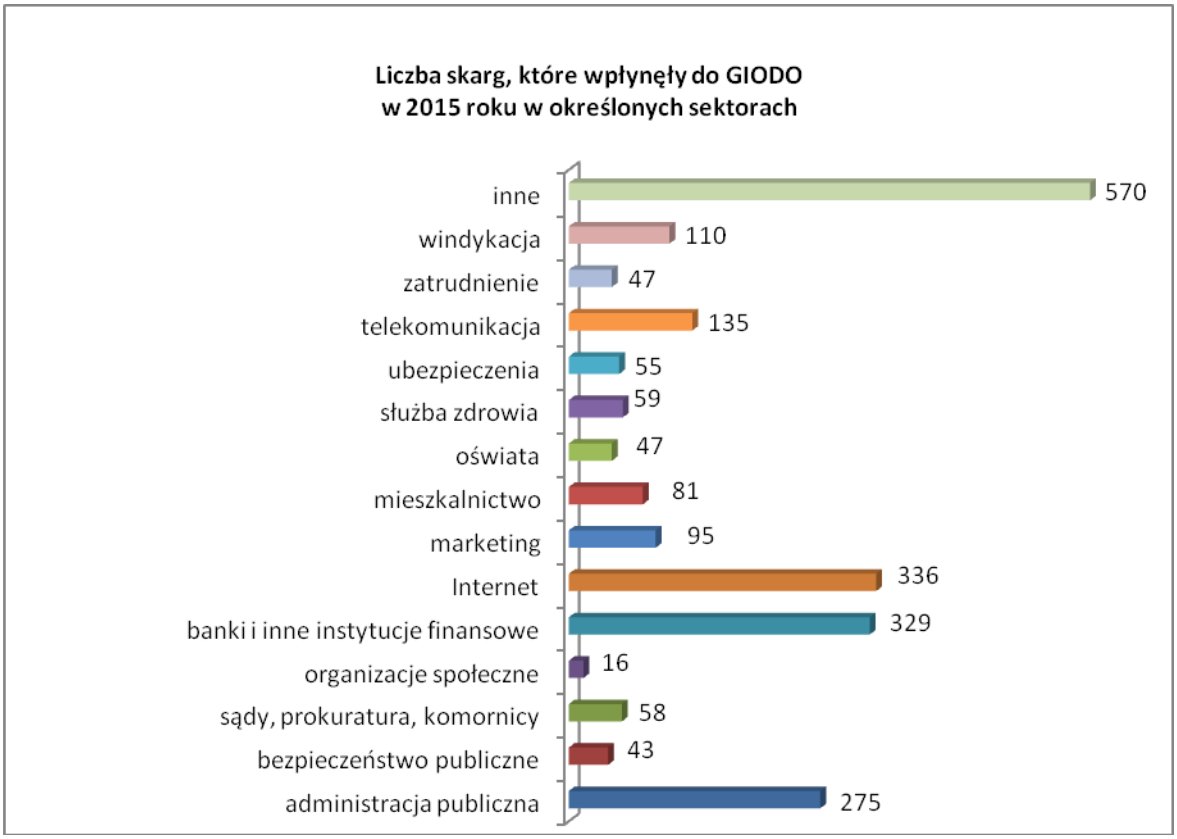
W analizowanym roku 2015 Generalny Inspektor Ochrony Danych Osobowych wystosował **80 wystąpień, w tym 57 wystąpień w trybie art. 19a ustawy o ochronie danych osobowych.**

W porównaniu z poprzednimi latami, **do 2014 r.** można zauważyć systematyczny **wzrost liczby skarg,** które wpływają do Biura GIODO. W roku 2010 wpłynęło 1114 skarg, w 2011 r. – 1271, w 2012 r. – 1593, w 2013 r. – 1879, w 2014 – 2481. Natomiast **w 2015 r. nastąpił spadek do liczby 2256 skarg**, choć liczba ta jest wciąż bardzo duża. Pomimo tego odnotowano wzrost liczby wydanych w 2015 r. decyzji w związku ze skargami o ok. 20% (646 decyzji wydanych przez DOLiS w 2015 r. przy 547 w 2014 r.). Jednocześnie podkreślenia wymaga, że wobec sztywnych ram prowadzenia postępowań określonych przepisami Kodeksu postępowania administracyjnego, Generalny Inspektor w dalszym ciągu boryka się z ogromną ilością napływających skarg i prowadzeniem postępowań administracyjnych, co przy stale rosnącej liczbie spraw w stosunku do możliwości organizacyjnych Biura GIODO rodzi szereg zagrożeń, jak np. bezczynność czy przewlekłość postępowania.

Zauważyć należy, iż liczba przypadków, w których stwierdzane były nieprawidłowości w procesie przetwarzania danych z roku na rok maleje. 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.

Porównanie liczby skarg wpływających w 2015 r. w poszczególnych sektorach w odniesieniu do roku 2014, pozwala dostrzec interesujące trendy. Pierwszym z nich był wzrost liczby skarg w sektorze dotyczącym administracji publicznej (rok 2014 - 249, rok 2015 - 275) oraz w sektorze odnoszącym się do działalności służby zdrowia (rok 2014- 47, rok 2015 – 59). Ponadto znaczący spadek odnotowano wśród skarg dotyczących obszaru Internetu (rok 2014 - 406, rok 2015 - 336), marketingu (rok 2014 – 153, rok 2015 - 95) oraz bezpieczeństwa publicznego (rok 2014 – 78, rok 2015 – 43). W niektórych sektorach liczba skarg była na porównywalnym poziomie, tj. w sektorze dotyczącym oświaty (rok 2014 - 63, rok 2015 - 55), w sektorze ubezpieczeń społecznych, majątkowych i osobowych (rok 2014 - 63, rok 2015 - 55), w sektorze dotyczącym telekomunikacji (rok 2014 – 134, rok 2015 - 135) oraz w sektorze dotyczącym windykacji (w obu okresach sprawozdawczych liczba skarg wyniosła

110). Ponadto stwierdzono istotną tendencję - w roku 2015 przestała wzrastać liczba skarg na banki i inne instytucje finansowe (rok 2014 – 354, rok 2015 – 329).



Wykres 38: ***Porównanie liczby skarg, które wpłynęły do Biura GIODO w 2015 r. w poszczególnych sektorach.***

Odnosząc się do zakresu tematycznego skarg rozpatrywanych przez Generalnego Inspektora Ochrony Danych Osobowych w omawianym 2015 roku, zasadniczo nie zauważa się znaczących zmian. W porównaniu z rokiem 2014 problemy pojawiające się we wpływających do Biura GIODO wnioskach uznać należy za tożsame. Najwięcej skarg, na przestrzeni ostatnich lat odnotować można w sektorze dotyczącym **działalności banków i innych instytucji finansowych, administracji publicznej czy też związanych z działalnością portali internetowych lub w samym Internecie.** Wraz ze wzrostem świadomości osób, których dane dotyczą, a które obserwują uważnie trendy związane z ochroną danych osobowych, zauważyć należy, iż np. po wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 13 maja 2014 r. (sygn. akt C-131/12), wzrosła liczba skarg na operatorów wyszukiwarek internetowych. Zaakcentować należy, że wraz z rozwojem nowych technologii z których często korzystają zarówno administratorzy danych, jak i osoby których

dane dotyczą, wzrosła również liczba skarg w tym zakresie. Korzystanie z nowoczesnych usług nierozerwalnie łączy się z udostępnianiem danych, a przy zastosowaniu odpowiedniej techniki, możliwość zidentyfikowania osoby nawet za pomocą szczątkowych informacji staje się coraz łatwiejsza, zwłaszcza wobec coraz powszechniejszego łączenia danych, pochodzących z różnych źródeł i wykorzystywanie ich do innych, w stosunku do pierwotnych, celów.

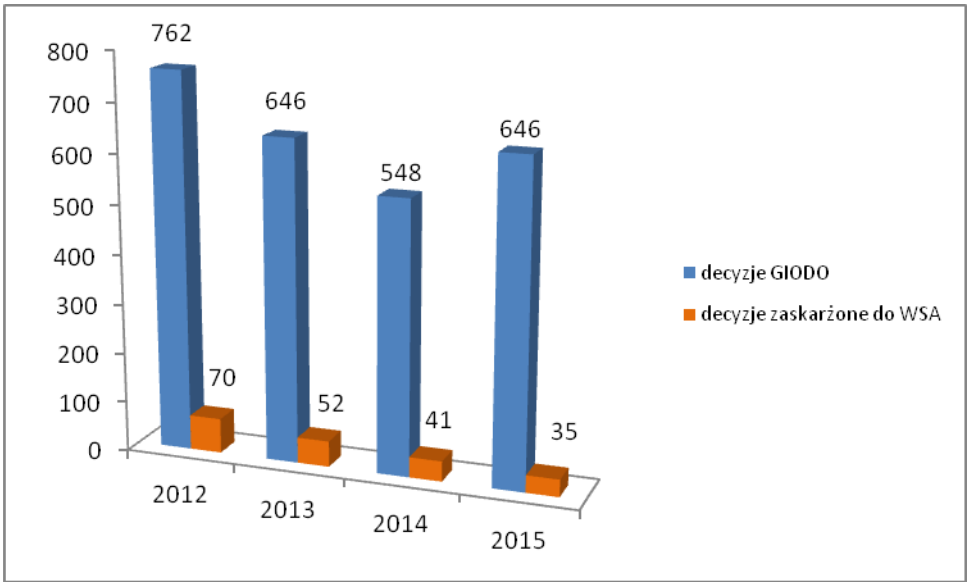
W przedmiocie naruszeń przepisów ustawy o ochronie danych osobowych można zaobserwować, iż najczęściej występującym naruszeniem był częściowy lub zupełny brak spełniania przez administratorów danych osobowych obowiązków informacyjnych wynikających z art. 33 ustawy, jak również nieterminowe realizowanie tych obowiązków przez administratorów danych. W szczególności podkreślenia wymaga, że prawo do informacji osób, których dane dotyczą jest istotne z punktu widzenia zapewnienia przez administratorów danych przejrzystości procesu przetwarzania danych osobowych. Każdorazowo w takich sytuacjach GIODO podejmował czynności mające na celu wyeliminowanie zaobserwowanych nieprawidłowości.

Ponadto wskazać również należy, iż systematycznie rośnie liczba wniosków o ponowne rozpatrzenie spraw, gdzie w 2015 r. wydano 129 decyzji w II instancji, co stanowi wzrost o ok. 20% w stosunku do roku ubiegłego (w 2014 r. 107 decyzji w II instancji).

Porównując statystki z roku 2015 r. do poprzedniego okresu sprawozdawczego zauważyć należy, iż znacząco wzrosła liczba spraw, w których organ skierował zawiadomienia o podejrzeniu popełnienia przestępstwa (z 10 zawiadomień z 2014 r. do 24 odnotowanych w 2015 roku).

Podsumowując należy odnotować, iż mimo dużej liczby skarg, które wpłynęły do GIODO w ostatnich latach, 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.

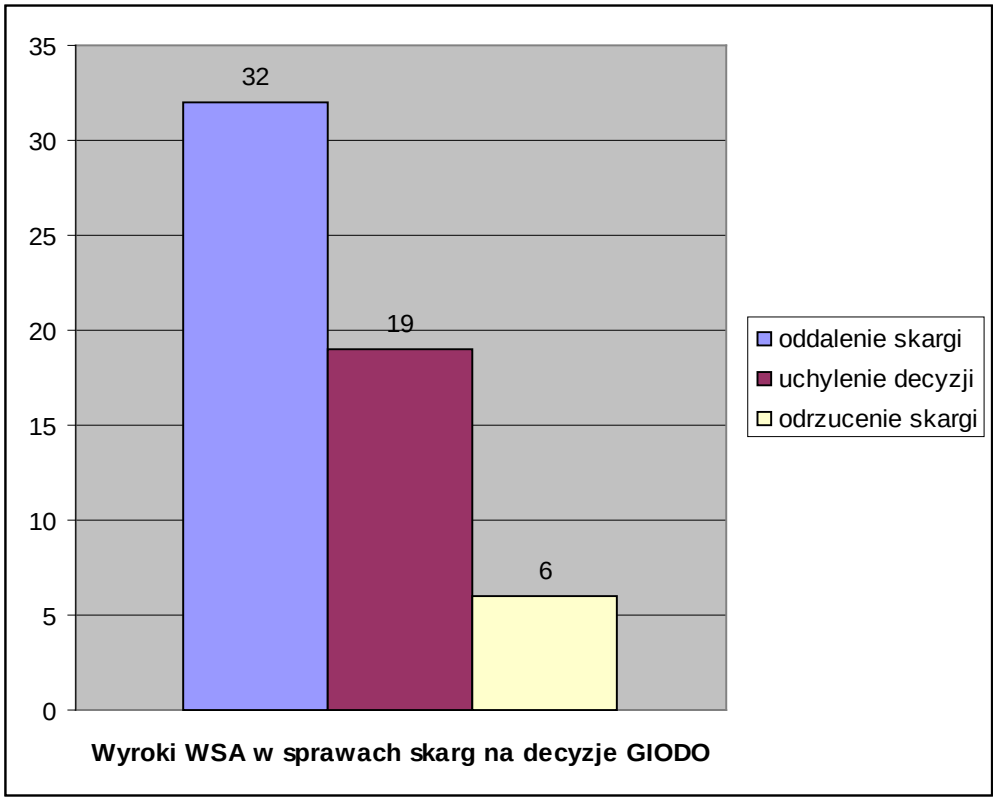
W postępowaniach zainicjowanych skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, w roku 2015 r. spośród **646** decyzji wydanych przez Departament Orzecznictwa, Legislacji i Skarg, Biura GIODO, **35** zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie [WSA]. W porównaniu z rokiem 2014, w którym 41 decyzji zostało zaskarżonych, oznacza to **spadek o 6 decyzji.**



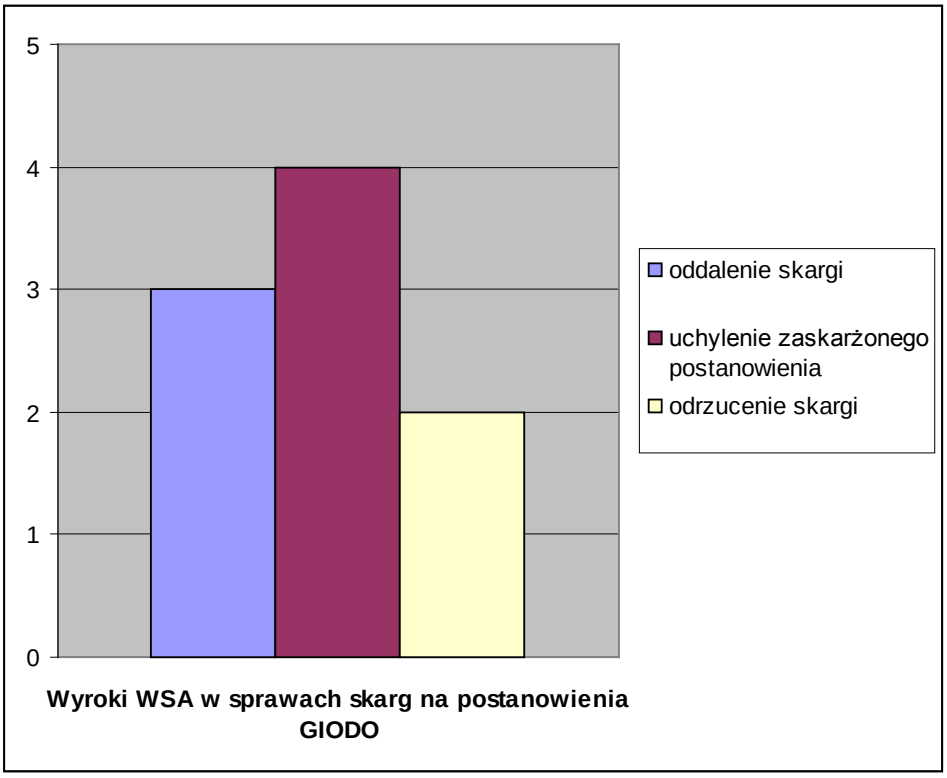
Wykres 39: ***Liczbowe zestawienie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych w latach 2012-2015 w związku z rozpatrywanymi skargami.***

Spośród 174 orzeczeń wydanych w sprawach związanych z działalnością skargową w 2015 rok, 127 orzeczeń rozstrzygało sprawy co do istoty, zaś pozostałych 47 orzeczeń stanowiły orzeczenia wydawane w toku prowadzonych przez sądy administracyjne postępowań. W analizowanym okresie 2015 roku Wojewódzki Sąd Administracyjny w Warszawie rozstrzygał sprawy co do istoty w 89 przypadkach.

Wśród orzeczeń wydanych przez WSA dotyczących skarg na decyzje GIODO w 2015 r. w **32** przypadkach Sąd orzekł o **oddaleniu** skargi na decyzję GIODO, zaś w **19** przypadkach **uchylił** zaskarżone decyzje. Ponadto w **6** sprawach WSA orzekł o **odrzuceniu** skargi spowodowanym nieuzupełnieniem, we wskazanym przez Sąd terminie, braków formalnych złożonych skarg.

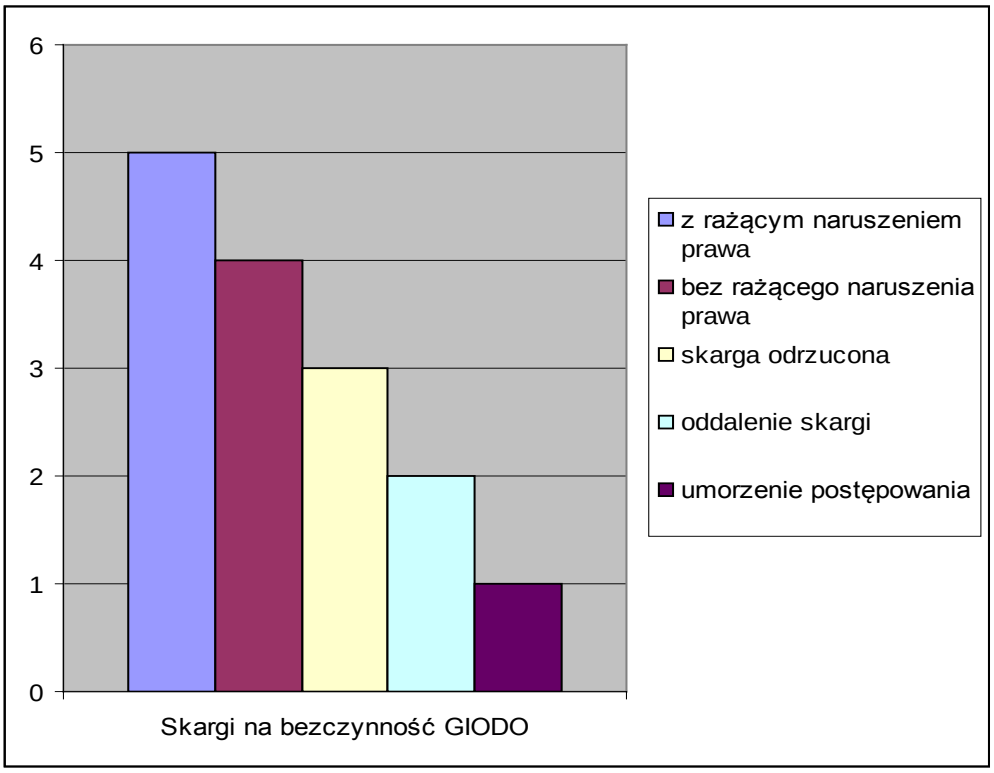


Wykres 40: ***Orzeczenia WSA wydane w 2015 r. w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych.***

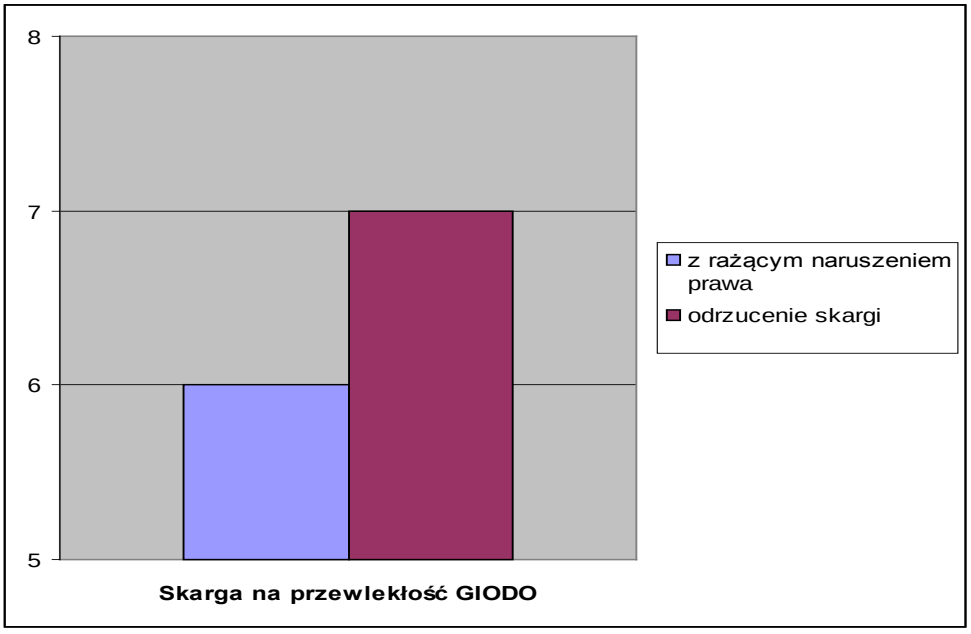


Wykres 41: ***Wyroki WSA w sprawach skarg na postanowienia Generalnego Inspektora Ochrony Danych Osobowych wydanych w sprawach prowadzonych w 2015 r.***

Na poniższych wykresach zilustrowano liczbę skarg na bezczynność i przewlekłość rozpatrywania spraw przez Generalnego Inspektora Ochrony Danych Osobowych w 2015 r.

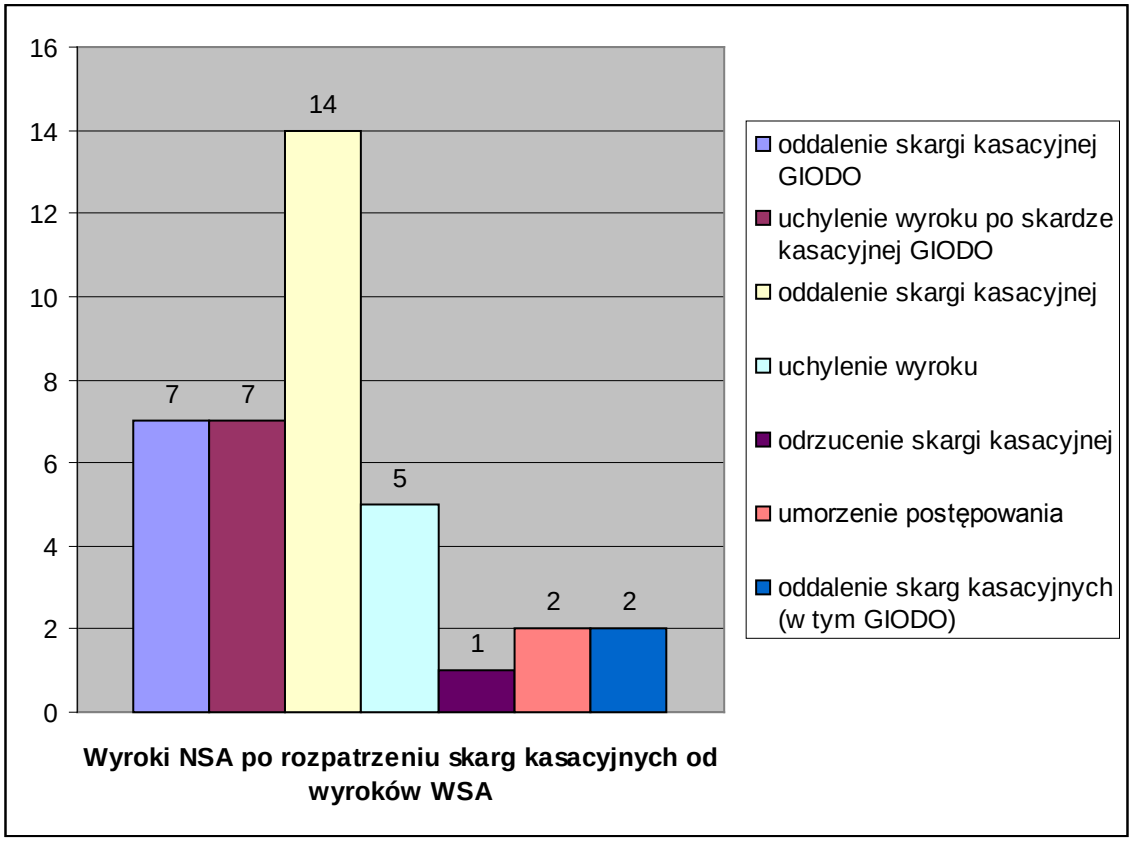


Wykres 42: ***Liczba skarg na bezczynność Generalnego Inspektora Ochrony Danych osobowych w sprawach prowadzonych w 2015 r.***



Wykres 43: ***Liczba skarg na przewlekłość postępowania w sprawach prowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych w 2015 r.***

Podkreślić należy, iż w **14** sprawach GIODO kierował do NSA skargi kasacyjne od wyroków WSA na skutek których w **7** sprawach zostały uchylone wyroki WSA, zaś w 7 przypadkach oddalono skargi kasacyjne GIODO. Spośród skarg kasacyjnych Skarżących podkreślić należy, iż w **16** przypadkach zostały one oddalone, w **5** sprawach wyroki WSA zostały uchylone, zaś **2** sprawy zostały umorzone. Ponadto wskazać należy, iż w 2 przypadkach skargi kasacyjne od wyroków złożył zarówno Generalny Inspektor, jak i strona postępowania administracyjnego. Natomiast w obu sytuacjach NSA oddalił skargi kasacyjne stron.



Wykres 44: ***Orzeczenia NSA wydane 2015 r. w związku ze skargami kasacyjnymi wniesionymi od wyroków WSA.***

Sfera prywatności jest objęta ochroną, do którego prawo wywodzić można w pierwszej kolejności z Konstytucji Rzeczypospolitej Polskiej (art. 47). Stąd w każdym przypadku, gdy konstruowane są przepisy, na podstawie których pozyskuje się, przechowuje i udostępnia dane osobowe - organ do spraw ochrony danych osobowych zwraca szczególną uwagę, aby nowo tworzone normy prawne odpowiadały standardom wyrażonym zarówno w Konstytucji Rzeczypospolitej Polskiej, jak i ustawie o ochronie danych osobowych. Jedną z

najważniejszych zasad wynikającą z ustawy ochronie danych osobowych jest bowiem konieczność zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, w oparciu o właściwy przepis prawa (art. 23, art. 27 i art. 26 ustawy). Powyższe zasady nabierają szczególnego znaczenia w przypadku przetwarzania danych przez podmioty publiczne, albowiem organy publiczne obowiązane są do działania jedynie na podstawie i w granicach prawa (art. 7 Konstytucji RP oraz art. 6 Kodeksu postępowania administracyjnego). Granice aktywności podmiotów publicznych wyznaczają wyłącznie normy prawne określające ich kompetencje, zadania, cele i tryb postępowania.

Analizując więc działalność **opiniotwórczą** Generalnego Inspektora Ochrony Danych Osobowych w 2015 r. podkreślić należy, iż proces legislacyjny wymaga udziału jego przedstawicieli w pracach nad projektami aktów prawnych na różnych etapach ich powstawania, począwszy od sporządzania opinii GIODO, poprzez udział w komisjach uzgodnieniowych organizowanych przez projektodawców celem utrzymania uwag GIODO, aż po udział w pracach Parlamentu, w przypadku przepisów o randze ustawy.

Odnotowania jednak wymaga coraz częściej pojawia się praktyka wprowadzania do projektów aktów prawnych istotnych zmian **już po zakończeniu uzgodnień międzyresortowych, najczęściej na etapie sejmowych prac legislacyjnych.** Jako typowy przykład może posłużyć projekt **ustawy o działalności ubezpieczeniowej i reasekuracyjnej**[276], do którego pierwotnie organ do spraw ochrony danych osobowych uwag nie zgłaszał[277].

Projekt ww. ustawy (druk sejmowy nr 3644), zawierał rozwiązania nowe, nieznane wcześniej, Generalnemu Inspektorowi Ochrony Danych Osobowych, który zakwestionował m.in. przepisy dotyczące prowadzenia przez ubezpieczeniowy Fundusz Gwarancyjny informatycznej bazy danych niezbędnej do przeciwdziałania przestępczości ubezpieczeniowej[278] – art. 102 a ustawy z dnia 22 maja 2003 roku o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze

[276] DOLiS-033-71/15

[277] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 24 marca 2015 roku o sygn. DOLiS-033-71/15/KK/23626 do Sekretarz Stanu w Ministerstwie Finansów.

[278] Pismo Generalnego Inspektora Ochrony Danych Osobowych z dnia 26 sierpnia 2015 roku o sygn. DOLiS-033-71/15/TG/78072 do Pani Poseł Zofii Czernow – ówczesnej Przewodniczącej Podkomisji nadzwyczajnej do rozpatrzenia rządowego projektu ustawy o działalności ubezpieczeniowej i reasekuracyjnej (druk nr 3644).

Ubezpieczycieli Komunikacyjnych[279] (ustawa o UFG), dodawany przez art. 453 pkt 10 projektu.

Ostatecznie w uchwalonej przez Parlament i podpisanej przez Prezydenta Rzeczypospolitej Polskiej **ustawie z dnia 11 września 2015 roku o działalności ubezpieczeniowej i reasekuracyjnej**[280] uwagi Generalnego Inspektora Ochrony Danych Osobowych zostały uwzględnione. Przepis odsyłający do uchwały Zgromadzenia Członków Ubezpieczeniowego Funduszu Gwarancyjnego w kwestii określenia zakresu oraz sposobu udostępniania przez Ubezpieczeniowy Fundusz Gwarancyjny zakładom ubezpieczeń informacji i danych, został usunięty, a w art. 486 ust. 3 tejże ustawy nałożono na Polską Izbę Ubezpieczeń obowiązek przekazania Ubezpieczeniowemu Funduszowi Gwarancyjnemu, danych i informacji zgromadzonych w bazach danych utworzonych na podstawie uchylanej ustawy o działalności ubezpieczeniowej. Mająca zaś być utworzona baza danych w zakresie niezbędnym do przeciwdziałania przestępczości ubezpieczeniowej została przekształcona w informatyczną bazę danych w zakresie niezbędnym do identyfikacji, weryfikacji i przeciwdziałania naruszeniu interesów uczestników rynku ubezpieczeniowego – art. 102 a ust. 1 ustawy o UFG, dodany przez art. 455 pkt 9 **ustawy o działalności ubezpieczeniowej i reasekuracyjnej**.

Organ do spraw ochrony danych osobowych wciąż oczekuje na dalsze prace nad **projektem założeń ustawy o monitoringu wizyjnym,** która w sposób prawidłowy będzie gwarantowała konstytucyjne wolności i prawa jednostki. Dotychczasowe propozycje legislacyjne w sposób niewystarczający określają uprawnienia osób obserwowanych, oznaczenia przestrzeni monitorowanych, jak również zakres udostępniania nagrań z monitoringu.

Rozumiejąc dążenie Państwa do usprawnienia procesów zarządzania posiadanymi systemami i zgromadzonymi w nich danymi osobowymi, jak również ułatwienia obywatelowi dostępu do tzw. e-usług w administracji, Generalny Inspektor Ochrony Danych Osobowych postuluje w swoich opiniach do poszczególnych projektów przepisów, czy też do założeń określonych rozwiązań, aby projektodawcy w należyty sposób uwzględniali rozwiązania alternatywne (to jest nie wykorzystujące danych osobowych w nadmiarze) na etapie założeń czy projektów aktów prawnych. Idea cyfryzacji często prowadzi bowiem do zbyt dużych

[279] Dz. U. z 2013 r. poz. 392 z późn. zm.
[280] Dz. U. z 2015 r. poz. 1844

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 2015 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. 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. Szereg unormowań uwzględniających ochronę danych osobowych 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. 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.

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 2015 r. zgłoszonych zostało do **rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych 31501 zbiorów, to jest o 11799 mniej niż w roku 2014. Wśród zgłoszonych w 2015 r. zbiorów do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, 15610 zbiorów pochodziło od podmiotów publicznych, zaś 15891 od podmiotów prywatnych.**

Podsumowując wszystkie zadania związane z rejestracją, w 2015 r. do Biura GIODO wpłynęło **54370 zgłoszeń zbiorów danych osobowych i powołania ABI, tj. o 25,5% więcej niż w 2014 r.,** w którym odnotowano tylko same zgłoszenia zbiorów do rejestracji (43300). W 2015 r. zarejestrowano **26268 zbiorów danych osobowych i ABI, tj. o 55,5% więcej niż w analogicznym okresie roku 2014,** w którym dokonano tylko rejestracji samych zbiorów danych osobowych (16870).

Realizacja zadań związanych z prowadzeniem rejestru zbiorów danych osobowych wymagała szybkiej i precyzyjnej analizy prawnej zgłoszeń oraz bardzo dobrej znajomości systemu prawa w Polsce. Chodzi tu nie tylko o przepisy ustawy o ochronie danych osobowych, ale także m.in. o obowiązujące przepisy kompetencyjne dotyczące podmiotów publicznych. Często sprawy miały złożony charakter i dotyczyły np. mega zbiorów prowadzonych przez organy administracji rządowej. Przykładem tego rodzaju zbioru był zgłoszony do rejestracji Generalnemu Inspektorowi w 2015 roku przez Ministra Zdrowia zbiór danych osobowych o nazwie „SYSTEM INFORMACJI MEDYCZNEJ P1 (SIMP1)" oraz zbiory dotyczące rejestrów centralnych lub zbiorów, co do których na przykład trudno wskazać podstawę prawną, mimo że prowadzone są przez podmioty publiczne. Często też w postępowaniu rejestracyjnym wyjaśniane były administratorom danych podstawowe pojęcia z zakresu ochrony danych osobowych. Dla przykładu, w toku postępowania prowadzonego w związku ze zgłoszeniem przez Agencję Restrukturyzacji i Modernizacji Rolnictwa zbioru danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych okazało się, że ustawowe pojęcie zbioru danych było przez wnioskodawcę błędnie utożsamiane z systemem informatycznym służącym do przetwarzania danych osobowych. Skutkowało to powstaniem wątpliwości, czy przedmiotowe zgłoszenie dotyczy jednego, czy też różnych zbiorów danych, w których dane są przetwarzane w odmiennych celach, na

podstawie różnych podstaw prawnych. Generalny Inspektor Ochrony Danych Osobowych poinformował wnioskodawcę, iż zgłoszenie zbioru danych do rejestracji powinno dotyczyć jednego zbioru danych osobowych, gdyż tylko wówczas jest możliwe dokonanie analizy zawartych w zgłoszeniu informacji i oceny procesu przetwarzania danych w zbiorze z punktu widzenia zasad przetwarzania danych osobowych, w tym m.in. zasady legalności i adekwatności. Ponadto Generalny Inspektor Ochrony Danych Osobowych zauważył, że jeden system informatyczny może służyć do przetwarzania danych osobowych w wielu zbiorach. Wybór środków i rozwiązań technicznych wykorzystywanych do przetwarzania danych należy do administratora danych, z tym zastrzeżeniem, że każdorazowo zobowiązany jest on przestrzegać przepisów o ochronie danych osobowych.

Zgodnie z art. 44 ust. 1 ustawy Generalny Inspektor Ochrony Danych Osobowych odmawia w drodze decyzji administracyjnej rejestracji zgłoszonego zbioru danych, m.in. w przypadku gdy przetwarzanie danych naruszałoby zasady określone w art. 23-28 ustawy. Jedną z nich jest zasada adekwatności, ujęta w art. 26 ust. 1 pkt 3 ustawy. Oznacza ona, że administrator danych przetwarzający dane osobowe jest w szczególności obowiązany zapewnić, aby dane te były adekwatne w stosunku do celów, w jakich są przetwarzane. Adekwatność (relewantność) powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi osobowymi a interesem administratora danych. Równowaga jest zachowana wówczas, gdy administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu ich przetwarzania. Zarząd Transportu Miejskiego w Warszawie zgłosił do rejestracji Generalnemu Inspektorowi zbiór danych o nazwie „SPERSONALIZOWANE WARSZAWSKIE KARTY MIEJSKIE DLA OSÓB UPRAWNIONYCH DO BEZPŁATNYCH PRZEJAZDÓW ŚRODKAMI LOKALNEGO TRANSPORTU ZBIOROWEGO M. ST. WARSZAWY”. Administrator poinformował o przetwarzaniu w przedmiotowym zbiorze danych osobowych pasażerów uprawnionych do bezpłatnych, bezterminowych przejazdów, które pozyskiwane były w drodze kopiowania dokumentów uprawniających do bezterminowych bezpłatnych przejazdów środkami lokalnego transportu zbiorowego. Wskazał przy tym, że celem przetwarzania tych danych jest ułatwienie pasażerom korzystania z bezpłatnych przejazdów środkami lokalnego transportu zbiorowego oraz umożliwienie wejścia do strefy biletowej metra bez konieczności posiadania przez pasażera oryginałów dokumentów uprawniających do bezpłatnych przejazdów w trakcie kontroli. Generalny Inspektor poinformował wnioskodawcę, że w związku z treścią

przepisów ustawy z dnia 15 listopada 1984 r. Prawo przewozowe (Dz. U. z 2012 r. poz. 1173 z późn. zm.) dotyczących uprawnień kontroli dokumentów przewozu osób lub bagażu przez przewoźnika lub organizatora publicznego transportu zbiorowego albo osobę przez niego upoważnioną, nie można uznać za uzasadnione przetwarzania danych pozyskiwanych poprzez kopiowanie dokumentów potwierdzających uprawnienia do bezpłatnych przejazdów we wskazanym w zgłoszeniu celu. Zarząd Transportu Miejskiego w Warszawie argumentował, iż prawo przewozowe zawiera jednocześnie regulacje umożliwiające przewoźnikowi lub organizatorowi przewozu określenie regulaminów przewozu i przepisów porządkowych regulujących zasady obsługi podróżnych, odprawy oraz przewozu osób i rzeczy. W szczególności administrator zwrócił uwagę na art. 4 i art. 15 ust. 5 Prawa przewozowego, informując, że na podstawie tych przepisów Rada m. st. Warszawy podjęła uchwałę Nr XXVI/858/2008 w sprawie opłat za usługi przewozowe środkami lokalnego transportu zbiorowego w m. st. Warszawie, zmiany uchwały w sprawie ulg za usługi przewozowe środkami lokalnego transportu zbiorowego w m. st. Warszawie oraz zmiany uchwały w sprawie regulaminu przewozu osób i bagażu środkami lokalnego transportu zbiorowego w m. st. Warszawie (Dz. Urz. Woj. Maz. Nr 52 poz. 1849 z późn. zm.). Zgodnie z § 5 ust. 2 w tytule II załącznika nr 3 do tej uchwały, na umotywowany wniosek pasażera posiadającego stałe uprawnienia do bezpłatnych przejazdów, Dyrektor ZTM lub osoba przez niego upoważniona może, po złożeniu przez pasażera niezbędnych dokumentów potwierdzających uprawnienie, wyrazić zgodę na ich zakodowanie na spersonalizowanej karcie zbliżeniowej. W takim przypadku, podczas kontroli biletowej, dokumentem potwierdzającym prawo do bezpłatnego przejazdu będzie spersonalizowana karta zbliżeniowa z zakodowanym uprawnieniem. Wnioskodawca podkreślił, że warunkiem uzyskania karty jest udokumentowanie posiadanych uprawnień, tj. złożenie kopii odpowiednich dokumentów.

Generalny Inspektor rozstrzygając sprawę stanął na stanowisku, że pozyskiwanie i dalsze przetwarzanie przez administratora wszystkich danych pasażerów zawartych w kopiach dokumentów potwierdzających uprawnienia do bezterminowych, bezpłatnych przejazdów środkami lokalnego transportu zbiorowego, którzy wnioskują o zakodowanie tych uprawnień na Spersonalizowanej Warszawskiej Karcie Miejskiej, będzie naruszało zasadę adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych, co stanowi przesłankę odmowy rejestracji zbioru danych, o której mowa w art. 44 ust. 1 pkt 2 ustawy. W konsekwencji Generalny Inspektor wydał decyzję, w której odmówił rejestracji zbioru danych osobowych o nazwie „SPERSONALIZOWANE WARSZAWSKIE KARTY

MIEJSKIE DLA OSÓB UPRAWNIONYCH DO BEZPŁATNYCH PRZEJAZDÓW ŚRODKAMI LOKALNEGO TRANSPORTU ZBIOROWEGO M. ST. WARSZAWY" i nakazał wnioskodawcy usunięcie z przedmiotowego zbioru danych osobowych nieadekwatnych do celu ich przetwarzania, tj. danych zawartych w kopiach dokumentów potwierdzających uprawnienia do bezterminowych bezpłatnych przejazdów środkami lokalnego transportu zbiorowego m.st. Warszawy oraz ograniczenie przetwarzania pozostałych danych zgromadzonych w tym zbiorze, wyłącznie do ich przechowywania do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu, stosownie do art. 44 ust. 4 ustawy o ochronie danych osobowych.

Zarząd Transportu Miejskiego w Warszawie złożył wniosek o ponowne rozpatrzenie sprawy. Zarzucił Generalnemu Inspektorowi naruszenie art. 27 ust. 2 pkt 1 ustawy polegające na błędnym uznaniu za niedopuszczalne przetwarzanie danych o stanie zdrowia, podczas gdy wyrażona na piśmie zgoda na przetwarzanie ww. danych stanowi przesłankę sankcjonującą przetwarzanie tych danych, a także naruszenie art. 26 ust. 1 pkt 3 ustawy polegające na uznaniu zakresu zbieranych danych jako nieadekwatnego do celu, podczas gdy ustalony przez administratora danych osobowych cel przetwarzania danych oraz przepisy prawa miejscowego uzasadniają zbieranie danych w postaci kopii dokumentów uprawniających do bezpłatnych przejazdów. Podnosząc powyższe zarzuty administrator wniósł o uchylenie zaskarżonej decyzji w całości, zaś w przypadku nieuwzględnienia powyższych zarzutów, z uwagi na nowe okoliczności, które wystąpiły po wydaniu decyzji, administrator wniósł o :

1. zarejestrowanie zbioru danych osobowych o nazwie „SPERSONALIZOWANE WARSZAWSKIE KARTY MIEJSKIE DLA OSÓB UPRAWNIONYCH DO BEZPŁATNYCH PRZEJAZDÓW ŚRODKAMI LOKALNEGO TRANSPORTU ZBIOROWEGO M. ST. WARSZAWY";
2. wyznaczenie terminu 6 miesięcy na usunięcie z powyższego zbioru, danych osobowych zawartych w kopiach dokumentów potwierdzających uprawnienia do bezpłatnych przejazdów środkami lokalnego transportu zbiorowego m. st. Warszawy.

Rozpatrując ponownie przedmiotową sprawę Generalny Inspektor Ochrony Danych Osobowych nie podzielił przedstawionej przez administratora argumentacji. W ocenie Generalnego Inspektora do zakodowania informacji na karcie i ułatwienia w ten sposób korzystania z bezpłatnych przejazdów osobom uprawnionym, wystarczające jest okazanie właściwych dokumentów i odpowiednie udokumentowanie tego wglądu. Nie ma potrzeby

pozyskiwania i przechowywania wszystkich danych osobowych zawartych w kopiach dokumentów, takich jak na przykład: orzeczenia właściwego organu, na podstawie przepisów prawa polskiego, o co najmniej częściowej niezdolności do pracy, orzeczenia zespołu orzekającego o niepełnosprawności, orzeczenia potwierdzające niepełnosprawność wydane przez zespół orzekający o stopniu niepełnosprawności lub orzeczenia wydane przez Komisję ds. Inwalidztwa i Zatrudnienia wraz z dokumentem poświadczającym, że niepełnosprawność spowodowana jest niepełnosprawnością intelektualną. Wykracza to bowiem poza rzeczywiste potrzeby wynikające z celu przetwarzania danych w powyższym zbiorze i narusza zasadę adekwatności, wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

Zdaniem administratora przetwarzanie danych osobowych pasażerów uprawnionych do bezpłatnych przejazdów, zwłaszcza w przypadku wyrażenia przez nich zgody na to przetwarzanie, nie może zostać uznane za nieadekwatne do celu. W przeciwnym wypadku pasażer, mimo wyrażonej jednoznacznej woli, nie mógłby dysponować swoimi danymi osobowymi.

Generalny Inspektor nie podzielił tego stanowiska. Podkreślił, że w jego opinii należy zawsze mieć na względzie, że zgoda może obejmować przetwarzanie danych jedynie w zakresie **wyznaczonym zasadą adekwatności**. Udzielenie zgody na przetwarzanie danych w zakresie szerszym niż wyznaczony zasadą adekwatności danych względem celu, nie może zostać zaaprobowane przez Generalnego Inspektora Ochrony Danych Osobowych. Zgodnie z art. 12 pkt 1 ustawy, do zadań Generalnego Inspektora należy kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Gdyby podzielić wyrażony przez administratora pogląd, to w konsekwencji należałoby stwierdzić, że organ do spraw ochrony danych osobowych, w sytuacji wyrażenia przez osobę, której dane dotyczą, zgody na ich przetwarzanie, nie może realizować jednego ze swoich podstawowych zadań przewidzianych w ustawie.

Administrator danych osobowych musi legitymować się jedną z przesłanek legalności przetwarzania danych osobowych. W odniesieniu do tzw. danych zwykłych zostały one wskazane w art. 23 ust 1 ustawy, zaś dla danych tzw. szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy – w art. 27 ust. 2 ustawy. Rada miasta stołecznego Warszawy podjęła między innymi na podstawie art. 4 i art. 15 ust. 5 ustawy z dnia 15 listopada 1984 r. Prawo przewozowe (Dz. U. z 2015 r. poz. 915) uchwałę Nr XXVI/858/2008 w sprawie opłat za usługi przewozowe środkami lokalnego transportu zbiorowego w m.st. Warszawie, zmiany uchwały w sprawie ulg za usługi przewozowe środkami lokalnego transportu zbiorowego w

m. st. Warszawie oraz zmiany uchwały w sprawie regulaminu przewozu osób i bagażu środkami lokalnego transportu zbiorowego w m.st. Warszawie (Dz. Urz. Woj. Maz. Nr 52 poz. 1849 z późn. zm.). Należy jednakże pamiętać, że dla uznania legalności przetwarzania określonej kategorii danych osobowych nie wystarczy legitymowanie się przez ich administratora którąś z przesłanek zawartych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy. Proces wykonywania na danych osobowych jakichkolwiek operacji jest zgodny z prawem dopiero wówczas, gdy odbywa się z uwzględnieniem wszystkich warunków, o których jest mowa w przepisach o ochronie danych osobowych. Ustawa o ochronie danych osobowych nakłada na administratora danych - poza powołanym wyżej obowiązkiem – m.in. obowiązek przestrzegania zasady adekwatności (relewantności) danych w stosunku do celów, dla jakich są one przetwarzane.

Generalny Inspektor nie przychylił się do wyrażonego przez Zarząd Transportu Miejskiego poglądu, jakoby treść przepisów uprawniających do bezpłatnych przejazdów uzasadniała kopiowanie dokumentów potwierdzających te uprawnienia i przechowywanie ich przez administratora danych. Organowi do spraw ochrony danych znana była wskazana przez wnioskodawcę linia orzecznicza Naczelnego Sądu Administracyjnego dotycząca utrwalania danych techniką kopiowania dokumentów. Generalny Inspektor w swojej decyzji wziął jednakże pod uwagę skutek posługiwania się tą techniką, to jest pozyskiwanie do zbioru wszystkich danych osobowych zawartych w tych dokumentach, co istotnie wykracza poza zakres adekwatny do wyznaczonego celu. O ile zrozumiała była konieczność weryfikacji przez wnioskodawcę dokumentów uprawniających podróżnego do bezpłatnych przejazdów przed wgraniem stosownego kodu na Spersonalizowaną Warszawską Kartę Miejską, to weryfikacja taka powinna następować wyłącznie poprzez okazanie stosownych, oryginalnych, a więc posiadających walor wiarygodności dokumentów i odpowiednie udokumentowanie tego wglądu. Nie jest natomiast konieczne pozyskiwanie i przechowywanie wszystkich danych osobowych zawartych w kopiach tych dokumentów, jako w istocie zbędnych dla realizacji zadań Zarządu Transportu Miejskiego w Warszawie.

Powyższe stanowisko wydaje się również podzielać sam administrator danych, informując o podjęciu działań zmierzających do wprowadzenia innego rozwiązania kwestii kodowania na SPERSONALIZOWANYCH WARSZAWSKICH KARTACH MIEJSKICH (SWKM) uprawnień do bezpłatnych biletów. Miałoby ono polegać na składaniu wniosków o wydanie przedmiotowej karty wraz z dokumentem potwierdzającym uprawnienie do ulgi. Następnie dokumenty podlegałyby weryfikacji pod względem autentyczności oraz zgodności

z wymienionymi w uchwale taryfowej i byłyby zwracane pasażerowi. W zbiorze będzie pozostawała jedynie informacja identyfikująca dany dokument (tytuł, numer, data wydania, organ wydający). Kopie wskazanych dokumentów nie będą przez administratora zachowywane.

Odnosząc się do alternatywnego wniosku podyktowanego nowymi okolicznościami, które wystąpiły po wydaniu decyzji, Generalny Inspektor wskazał, że przetwarzanie danych w zbiorze danych osobowych o nazwie „SPERSONALIZOWANE WARSZAWSKIE KARTY MIEJSKIE DLA OSÓB UPRAWNIONYCH DO BEZPŁATNYCH PRZEJAZDÓW ŚRODKAMI LOKALNEGO TRANSPORTU ZBIOROWEGO M. ST. WARSZAWY" nadal następuje z naruszeniem zasady adekwatności, co wypełnia przesłankę wydania decyzji o odmowie rejestracji zbioru danych, na podstawie art. 44 ust. 1 pkt 2 w związku z art. 26 ust. 1 pkt 3 ustawy. Kwestionowane dane nie zostały usunięte z wyżej wskazanego zbioru. W przypadku dokonania jego wpisu do ogólnokrajowego jawnego rejestru zbiorów danych osobowych oraz wyznaczenia terminu 6 miesięcy na usunięcie danych zawartych w kopiach dokumentów, doszłoby do sytuacji, w której Generalny Inspektor zaaprobowałby czasowe naruszanie przez administratora przepisów ustawy o ochronie danych osobowych, a także poddał w wątpliwość zasadność wydanej w pierwszej instancji decyzji o odmowie rejestracji przedmiotowego zbioru. Z powyższych względów została ona utrzymana w mocy przez Generalnego Inspektora Ochrony Danych Osobowych.

W odniesieniu do zadania Generalnego Inspektora Ochrony Danych Osobowych, jakim jest **rejestracja ABI**, w dniu 10 czerwca 2015 r. wydane zostało zarządzenie nr 08/2015 Generalnego Inspektora Ochrony Danych Osobowych, którym wprowadzono do *Jednolitego rzeczowego wykazu akt Biura Generalnego Inspektora Ochrony Danych Osobowych* nowe klasy: 406 – Akta rejestrowe administratorów bezpieczeństwa informacji i 407 – Zaświadczenia o rejestracji administratorów bezpieczeństwa informacji. W związku z tym, Departament Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych opracował szablony podstawowych pism, jakie będą kierowane do administratorów danych w toku postępowań rejestracyjnych dotyczących administratorów bezpieczeństwa informacji oraz szablon zaświadczenia o zarejestrowaniu administratora bezpieczeństwa informacji.

W celu maksymalnego usprawnienia obsługi zgłoszeń do rejestracji powołania administratora bezpieczeństwa informacji obarczonych brakami formalnymi oraz załatwiania wniosków administratorów danych i administratorów bezpieczeństwa informacji o wydanie

zaświadczenia o zarejestrowaniu ABI, szablony te zostały zamieszczone w *systemie rejestr ABI*, służącym do prowadzenia ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji. W zgłoszeniu powołania administratora bezpieczeństwa informacji, w zakładce „Załączniki", umieszczona została opcja wyboru szablonu. Wybór szablonu skutkuje utworzeniem projektu pisma z zaciągniętymi z systemu danymi, w formacie umożliwiającym pracownikowi rozpatrującemu zgłoszenie edycję danego dokumentu. Po wprowadzeniu zmian dokument byłby drukowany i zapisywany w systemie, co pozwala na sprawne ustalenie, na jakim etapie znajduje się sprawa.

Realizacja nowego zadania związanego z prowadzeniem **rejestru administratorów bezpieczeństwa informacji,** wymagała dokonywania na bieżąco analiz natury prawnej. W toku prowadzonych postępowań, jak również w związku z zapytaniami od administratorów danych, pojawiały się wciąż nowe kwestie wymagające rozstrzygnięcia. Często dotyczyły one skutków prawnych przepisów przejściowych ustawy o ułatwieniu wykonywania działalności gospodarczej. Co więcej lakoniczność tych przepisów skutkowała również wieloma wątpliwościami w zakresie postępowań rejestracyjnych dotyczących zbiorów danych osobowych.

Postępowania rejestracyjne dotyczące **zgłoszeń zbiorów danych złożonych przed dniem 1 stycznia 2015 r.,** prowadzone są zgodnie z przepisami dotychczasowymi (art. 36 ustawy o ułatwieniu wykonywania działalności gospodarczej). Zgłoszenie zbioru danych dokonane nie na obowiązującym formularzu lub brak w treści zgłoszenia informacji określonych w art. 41 ust. 1 ustawy o ochronie danych osobowych, stanowiło przesłankę wydania decyzji o odmowie rejestracji zbioru, o której mowa w art. 44 ust. 1 pkt 1 tej ustawy. W decyzjach o odmowie rejestracji zbioru w takich przypadkach zawarty był nakaz ograniczenia przetwarzania danych zgromadzonych w zbiorze wyłącznie do ich przechowywania do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu. W związku z powyższym konieczne stało się rozstrzygnięcie wątpliwości dotyczącej przypadków, w których z treści pierwotnego zgłoszenia wynika, że ponownie zgłoszony do rejestracji zbiór nie zostanie wpisany do rejestru zbiorów danych osobowych (nie są w nim przetwarzane dane szczególnie chronione, a zbiór prowadzony jest wyłącznie w postaci papierowej lub administrator danych zgłosił do rejestracji administratora bezpieczeństwa informacji). Bowiem brak było podstaw do wpisania do ogólnokrajowego rejestru, zbioru danych zgłoszonego po dniu 1 stycznia 2015 r., gdy zbiór ten był objęty nowym zwolnieniem z obowiązku rejestracji, jak również w sytuacji, gdy było to ponowne zgłoszenie, o którym

mowa w art. 44 ust. 4 ustawy o ochronie danych osobowych. W takim przypadku Generalny Inspektor wydawał decyzję o odmowie rejestracji oraz umorzeniu postępowania w części dotyczącej wydania nakazu ograniczenia przetwarzania danych zawartych w zbiorze do czasu jego rejestracji po ponownym zgłoszeniu, z uwagi na bezprzedmiotowość postępowania w tej części.

Należy również podkreślić, że zgłoszenie powołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi, nie stanowiło dla administratora danych podstawy do wystąpienia z wnioskiem o wykreślenie z ogólnokrajowego, jawnego rejestru zbiorów danych uprzednio do niego wpisanych zbiorów danych. Brak jest podstawy prawnej do wykreślania (na wniosek albo z urzędu) zarejestrowanych zbiorów danych, a informacje o nich zawarte w rejestrze zbiorów danych osobowych prowadzonym przez Generalnego Inspektora, służą potwierdzaniu spełniania przez administratorów danych przepisów Rozdziału 6 ustawy o ochronie danych osobowych obecnie i w przeszłości.

W celu poprawy dostępu do informacji na temat administratorów bezpieczeństwa informacji, w Biurze GIODO powstał projekt kompleksowej koncepcji informacji związanych z funkcjonowaniem ABI w nowym stanie prawnym. Zaproponowano schemat/layout zakładki ABI, który pozwoliłby na uproszczenie dostępu do informacji o ABI, zgromadzenie ich w jednym łatwo dostępnym miejscu i zapewnienie większej dokładności i przekrojowości oferowanych informacji.

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. Jest m.in. autorem ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", który ma na celu uwrażliwienie nauczycieli i uczniów na zagrożenia, jakie dla ochrony danych osobowych i prywatności istnieją w codziennym korzystaniu z Internetu. Statystycznie rocznie przystępuje do niego ponad 200 placówek, a w jego realizację włączonych jest ok. 4000 nauczycieli oraz 30000 uczniów w całej Polsce. W roku szkolnym 2015/2016 realizowana jest szósta edycja tego projektu, w której uczestniczy 250 placówek.

Uczestniczy także 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 i warsztaty adresowane głównie do przedstawicieli administracji rządowej i samorządowej oraz przedstawicieli instytucji publicznych. Współpracuje z 17 szkołami wyższymi w Polsce, 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 2015 roku do grona szkół wyższych, z którymi GIODO zawarł porozumienia o współpracy, dołączył Wydział Prawa i Administracji Uniwersytetu Warszawskiego, Wyższa Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, Instytut Nauk Prawnych Polskiej Akademii Nauk oraz Wyższa Szkoła Policji w Szczytnie.

Ponadto, w ramach współpracy GIODO z innymi instytucjami i organizacjami, podpisane zostały porozumienia o wspólnym działaniu na rzecz podnoszenia standardów ochrony danych osobowych i prawa do prywatności a także wypracowane zostały kodeksy dobrych praktyk w dziedzinie ochrony danych osobowych.

GIODO podejmuje ponadto szereg działań w ramach współpracy międzynarodowej, do których 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 GIODO 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).

Aktywność GIODO na przestrzeni blisko 18 lat funkcjonowania urzędu w zauważalny sposób wpłynęła na podniesienie poziomu świadomości społeczeństwa w kwestiach

związanych z ochroną danych osobowych. Jest to widoczne zarówno jeśli chodzi o obecność tych zagadnień w debacie publicznej, jak i coraz liczniej kierowane do organu skargi dotyczące naruszenia przepisów o ochronie danych osobowych oraz zapytania z prośbą o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, bądź sygnalizujących różnego rodzaju problemy interpretacyjne związane z ich przestrzeganiem.

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

W ostatnich latach znacząco wzrosło obciążenie urzędu, szczególnie biorąc pod uwagę liczbę skarg na nieprawidłowości w związku z przetwarzaniem danych osobowych, otrzymywanych przede wszystkim od osób, których dane dotyczą. Co roku do Biura GIODO wpływa rocznie ok. 4,5 tysiąca pytań z prośbą o interpretację przepisów prawa i blisko 2,5 tysiąca skarg. Dla porównania – w 2007 r. było to odpowiednio ok. 1,7 tysiąca pytań i niecałe 800 skarg. Innym ważnym zadaniem, a jednocześnie wyzwaniem dla GIODO jest rejestracja zbiorów danych osobowych. W 2015 r. do rejestracji zgłoszono ponad 31 tysięcy zbiorów, podczas gdy w 2007 r. było to zaledwie niecałe 5 tysięcy. Ponadto od 2015 r. Biuro GIODO zajmuje się również rejestracją administratorów bezpieczeństwa informacji. Zgodnie bowiem z nowelizacją ustawy o ochronie danych osobowych, jeżeli administrator danych skorzysta z przysługującego mu uprawnienia i powoła administratora bezpieczeństwa informacji, ma 30 dni od dnia powołania ABI na zgłoszenie tego faktu do rejestracji Generalnemu Inspektorowi.

Tymczasem zatrudnienie w latach 2007-2015 wzrosło jedynie o ok. 25% (ze 120 zatrudnionych na dzień 31 grudnia 2007 r. do 150 na dzień 31 grudnia 2015 r.). Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2007 r. wynosił: 12 391 tys. zł (w tym 8 152 tys. zł przeznaczone na wynagrodzenia), a w ustawie budżetowej na 2015 r. – 16 749 tys. zł (w tym 10 156 tys. zł na wynagrodzenia).

Obserwując wzrastającą liczbę spraw, którymi organ obowiązany jest się zajmować, uzasadniony wydaje się być wniosek, że bez pewnych zmian systemowych coraz trudniej będzie sprostać wszystkim wyzwaniom. Szansą na podniesienie poziomu realnego przestrzegania przepisów jest wzmocnienie pozycji organu ochrony danych osobowych i przyznanie mu kompetencji do nakładania kar finansowych, co wynika z planowanej reformy unijnych regulacji. Obecnie GIODO nie posiada uprawnień do nakładania kar finansowych, co w praktyce niejednokrotnie wpływa negatywnie na skuteczność działań.

Sytuację dodatkowo komplikuje fakt, iż urząd nie posiada oddziałów terenowych i dysponuje jedynie 14 inspektorami (przeprowadzającymi działania kontrolne zgodnie z art. 12 pkt 1 ustawy o ochronie danych osobowych) w skali kraju. Dla porównania, Państwowa Inspekcja Pracy (PIP) posiada 1700 inspektorów oraz kilka tysięcy społecznych inspektorów pracy. Z kolei system ochrony praw konsumentów opiera się na miejskich i powiatowych rzecznikach konsumentów.

W związku z powyższym, zdaniem organu, w praktyce musi zostać wzmocniona również pozycja obecnych administratorów bezpieczeństwa informacji (ABI). Zgodnie z nowym unijnym rozporządzeniem będą to inspektorzy ochrony danych osobowych (*data protection officers – DPO*). Generalny Inspektor widzi realną potrzebę współpracy z tymi podmiotami. Obecnie zarejestrowanych jest 15531 ABI, 8000 kolejnych zgłoszeń czeka na rejestrację i liczba ta sukcesywnie rośnie.

Z dniem 1 stycznia 2015 r. weszły w życie przepisy znowelizowanej ustawy o ochronie danych osobowych, określające m.in. zadania administratora bezpieczeństwa informacji (ABI). Decyzja o powołaniu ABI należy 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. Niepowołanie administratora bezpieczeństwa informacji skutkuje tym, że w razie zaistnienia nieprawidłowości związanych z przetwarzaniem danych osobowych to administrator danych osobowych (czyli np. minister w przypadku rejestrów o charakterze centralnym) ponosi pełną odpowiedzialność z tego tytułu – również karną, na podstawie przepisów Rozdziału 8 ustawy o ochronie danych osobowych.

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. Niniejsza sugestia znajduje szczególne zastosowanie wobec administratorów danych **z sektora publicznego**, który na mocy przepisów ogólnego rozporządzenia o ochronie danych objęty będzie zasadą obowiązkowego powoływania inspektora ochrony danych.

Zgodnie z obowiązującymi od początku 2015 r. przepisami znowelizowanej ustawy o ochronie danych osobowych, jednym z zadań ABI jest obecnie wykonywanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych. W ocenie organu działalność ABI w tym zakresie może pomóc w zapewnieniu wyższego poziomu ochrony danych osobowych. Pod tym względem Generalny Inspektor widzi w administratorach bezpieczeństwa informacji swoich partnerów, a nawet podmioty, które w pierwszej kolejności mogłyby reagować na nieprawidłowości dotyczące przetwarzania danych u administratorów danych osobowych, którzy ich powołali. Konieczne jest jednak do tego odpowiednie przygotowanie merytoryczne oraz wola współpracy z organem ochrony danych osobowych.

Wzmocnienie poziomu ochrony w ramach struktur administratorów danych osobowych i administratorów bezpieczeństwa informacji jest potrzebne również ze względu na fakt, iż Generalny Inspektor bywa traktowany jak podmiot do świadczenia obsługi prawnej administratorów danych osobowych, zarówno z sektora publicznego, jak i prywatnego. Biuro często otrzymuje pytania dotyczące rozwiązań organizacyjnych, jakie powinien przyjąć administrator danych, czy podejmowanych przez niego decyzji. Tymczasem takie rozstrzygnięcia nie leżą w kompetencji GIODO, bowiem to administrator danych osobowych, jako podmiot decydujący o celach i środkach przetwarzania danych osobowych, powinien zapewniać przestrzeganie przepisów o ochronie danych osobowych oraz stosować odpowiednie do swojej struktury, realizowanych zadań, zakresu przetwarzanych danych osobowych (zarówno kategorie danych, jak i skala ich przetwarzania) środki techniczne i organizacyjne w tym zakresie, w tym w postaci administratora bezpieczeństwa informacji. GIODO ma kompetencje do kontroli przyjętych rozwiązań, a nie zastępowania podmiotów, które powinny przestrzegać zasad ochrony danych osobowych w realizacji ich obowiązków.

Doświadczenie Generalnego Inspektora pokazuje również, ż pomimo istnienia w przepisie art. 12 pkt 5 stosownej kompetencji, nie wszystkie projekty aktów normatywnych istotnych z punktu widzenia ochrony danych osobowych są przedstawiane organowi do zaopiniowania (dotyczy to zarówno projektów rozporządzeń, ustaw, jak i umów międzynarodowych). Bywa, że GIODO jest włączany w proces legislacyjny dopiero na etapie

prac parlamentarnych. Zdarza się również, że jest całkowicie pomijany podczas konsultacji treści projektów, które bezpośrednio wiążą się z kwestią ochrony danych osobowych. Konieczne jest zatem monitorowanie na bieżąco przez pracowników Biura wszystkich projektów aktów normatywnych, które mogą mieć związek z tym zagadnieniem, co często jest zadaniem wysoce utrudnionym z uwagi na ich ilość.

Rola organu w procesie legislacyjnym bywa ponadto niewłaściwie rozumiana. W odpowiedzi na zgłaszane zastrzeżenia z punktu widzenia zgodności z ustawą o ochronie danych osobowych, projektodawcy często oczekują od GIODO sformułowania gotowych propozycji brzmienia przepisów. Tymczasem organ do spraw ochrony danych osobowych może jedynie wskazać kierunki potencjalnych rozwiązań i pełnić funkcję doradczą, natomiast sformułowanie konkretnych rozwiązań legislacyjnych należy do projektodawcy – tym bardziej, że to projektodawca powinien dysponować wiedzą dotyczącą celów przetwarzania danych oraz na temat tego, do jakiego rodzaju danych potrzebny jest dostęp biorąc pod uwagę realizację zadań wynikających z projektowanych przepisów. Pierwsza ocena w tym zakresie powinna należeć do administratorów bezpieczeństwa informacji funkcjonujących w ramach poszczególnych resortów. Tego rodzaju analiza powinna zostać przeprowadzona z uwzględnieniem wynikających z ogólnego rozporządzenia o ochronie danych koncepcji *privacy by default* oraz *privacy by design* i dokonaniem oceny skutków projektowanych rozwiązań na prywatność jednostek (*privacy impact assessment*).

Generalny Inspektor Ochrony Danych Osobowych może zatem wyrazić opinię co do zgodności projektowanych przepisów z przepisami ustawy ochrony danych osobowych i pełnić w procesie formułowania przepisów funkcję partnera projektodawcy, a nie kolejnego twórcy przepisów. GIODO jako organ niezależny, nieznajdujący się w strukturze rządowej, nie posiada również inicjatywy ustawodawczej, co ewentualnie uzasadniałoby oczekiwania dotyczące przedstawiania przez niego poprawek legislacyjnych.

Ograniczone możliwości działania GIODO wynikają jednak nie tylko z wyżej wspomnianego braku inicjatywy ustawodawczej. Generalnemu Inspektorowi nie przysługuje także prawo do złożenia do Trybunału Konstytucyjnego wniosku o stwierdzenie niezgodności przepisów prawa wydawanych przez centralne organy państwowe, z Konstytucją RP, ratyfikowanymi umowami międzynarodowymi i ustawami. W znaczący sposób ogranicza to możliwość działania w przypadku, gdy zostały uchwalone przepisy, co do których na etapie prac rządowych lub parlamentarnych organ zgłaszał uwagi dotyczące ich niezgodności z Konstytucją i ustawą o ochronie danych osobowych. Organ nie posiada ponadto uprawnień do

skierowania do Naczelnego Sądu Administracyjnego wniosku o podjęcie uchwały w celu wyjaśnienia przepisów prawnych prawa materialnego lub procesowego, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych. Na pozycję organu negatywnie oddziałuje także brak jego umocowania w przepisach Konstytucji RP – tak jak ma to miejsce w przypadku Rzecznika Praw Obywatelskich czy Rzecznika Praw Dziecka.

W podsumowaniu podkreślenia wymaga, że przetwarzanie danych osobowych z zachowaniem odpowiednich środków ostrożności i z poszanowaniem zasad wynikających z obowiązujących przepisów prawa jest konieczne nie tylko ze względu na ochronę prywatności jednostek, ale także z uwagi na zapewnienie bezpieczeństwa państwa, rozumianego jako bezpieczeństwo przepływu informacji. Służy temu celowi przedstawiony szeroki zakres obowiązków spoczywających na Generalnym Inspektorze Ochrony Danych Osobowych, oraz ilustruje różnorodność zagadnień, z którymi urząd spotyka się w praktyce. Przez blisko 18 lat obowiązywania ustawy o ochronie danych osobowych w polskim porządku prawnym obszar działalności organu znacząco ewoluował, przy niezmiennych, a zatem ograniczonych możliwościach działania organu i nieadekwatnej liczbowo obsadzie kadrowej. W celu zwiększenia efektywności działania urzędu, co jest potrzebne zwłaszcza z uwagi na opisane wyżej wyzwania związane z rozwojem technologii i przyszłe, ale nieodległe, rozwiązania prawne na poziomie rozporządzenia ogólnego, konieczne jest nowe spojrzenie na rolę Generalnego Inspektora i przekształcenie jej tak, by odpowiadała zarówno wymogom wynikającym z przepisów prawa Unii Europejskiej, jak i potrzebom osób, których dane dotyczą. Niewątpliwie jest to ogromne wyzwanie, które stoi zarówno przed podmiotami opracowującymi projekty aktów prawnych, ustawodawcą, jak również adresatami tychże przepisów. Jego realizacja nie będzie jednak możliwa bez wprowadzenia stosownych zmian w przepisach prawa oraz bez dysponowania odpowiednimi środkami do urzeczywistnienia tychże zadań. Jednocześnie organ deklaruje chęć współpracy i aktywnego udziału w działaniach mających na celu doprowadzenie do powstania konkretnych rozwiązań prawnych.

Szybki rozwój nowych technologii przyniósł nowe wyzwania w zakresie ochrony danych osobowych. Skala pozyskiwania, gromadzenia i wymiany danych osobowych osiągnęła niebotyczne rozmiary. Z jednej strony jest to możliwe m.in. dzięki nowym, ciągle rozwijanym, technologiom, z których korzystają zarówno podmioty władzy publicznej, jak i przedsiębiorstwa prywatne. Z drugiej strony, osoby fizyczne coraz aktywniej udostępniają wiele informacji ze swego życia prywatnego, a nawet intymnego, co powoduje, że stają się one publicznie dostępne. Fakt, że umieszczamy takie dane w Internecie może prowadzić do

wniosku, że mamy do niego zaufanie i nie zdajemy sobie sprawy z zagrożeń dla bezpieczeństwa danych osobowych, jakie ze sobą niesie zjawisko funkcjonowania tej globalnej sieci.

Korzystanie z nowoczesnych usług wręcz nierozerwalnie łączy się z udostępnianiem danych osobowych. Płatności przy użyciu kart kredytowych, zakupy przez Internet, korzystanie z poczty elektronicznej, wyszukiwarek i portali społecznościowych czy używanie telefonów komórkowych – każda z tych zaledwie przykładowo wskazanych czynności wiąże się z udostępnianiem informacji na nasz temat. Informacje te mają różny stopień szczegółowości, różny charakter – od najdrobniejszych po najbardziej intymne, jednak przy obecnym poziomie rozwoju technologicznego do identyfikacji konkretnej osoby nie jest już niezbędne znanie jej imienia i nazwiska. Podkreślić przy tym należy, że 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. Przy zastosowaniu odpowiedniej techniki, możliwość zidentyfikowania osoby nawet za pomocą szczątkowych informacji staje się coraz łatwiejsze, zwłaszcza wobec coraz powszechniejszego łączenia danych pochodzących z różnych źródeł i wykorzystywania ich do nowych, w stosunku do pierwotnych, celów.

Wrażenie anonimowości w Internecie obecnie pozostaje tylko iluzją. W rzeczywistości już samo wejście na stronę internetową wiąże się z wytwarzaniem i gromadzeniem danych pozwalających na identyfikację bądź „wyodrębnienie" konkretnej osoby. Wszelkie rodzaju aktywność w sieci – wyszukiwane hasła, odwiedzane strony, kupione produkty, poszczególne kliknięcia i wysyłane czy publikowane przez użytkownika informacje – są rejestrowane w postaci tzw. cyfrowych śladów oraz gromadzone na serwerach właścicieli stron i dostawców Internetu. Źródłem informacji na temat konkretnych osób są również tzw. ciasteczka, czyli pliki *cookies*. Należy jednak poczynić rozróżnienie między plikami zapisywanymi na dysku użytkownika podczas korzystania ze stron internetowych, które pozwalają na zapamiętywanie np. haseł czy danych z wypełnianych formularzy, a plikami, których celem jest śledzenie aktywności internautów – tzw. *tracking cookies*.

Współcześnie dane osobowe stały się rodzajem „cyfrowej waluty", którą użytkownicy Internetu muszą płacić za korzystanie z różnego rodzaju – w teorii darmowych – usług. Za pozyskiwanymi i analizowanymi w ten sposób informacjami stoi ogromna wartość ekonomiczna. Według badań wartość danych obywateli UE w 2011 r. wynosiła 315 mld euro. Do 2020 r. może ona wzrosnąć do blisko 1 bln euro rocznie. Jednocześnie w ogromnym

tempie rośnie ilość dostępnych na rynku informacji o osobach – dla porównania, dziś, w ciągu zaledwie dwóch dni produkowane jest tyle danych, ile ludzkość wytworzyła do roku 2003.

Nic więc dziwnego, że obowiązujące w zakresie ochrony danych osobowych prawo przestało nadążać za rzeczywistością. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, która stanowi podstawę dla krajowych przepisów dotyczących ochrony danych osobowych, pochodzi z 1995 r. Tymczasem, 20 lat temu dostęp do Internetu posiadało zaledwie 0,8% światowej populacji, a dwa obecnie najpopularniejsze portale – Google i Facebook – miały powstać odpowiednio 3 i 9 lat później.

Wraz z ciągłym rozwojem technologii mnożą się nowe zagrożenia związane z ochroną danych osobowych przetwarzanych w coraz to szerszym zakresie oraz na coraz to nowe sposoby. Jak wynika z przedstawionych w tym roku badań Eurobarometru, zaufanie obywateli do środowisk cyfrowych pozostaje na niskim poziomie. Dwie trzecie respondentów (67%) odpowiedziało, że martwią się faktem, iż nie mają kontroli nad informacjami, które podają w Internecie, podczas gdy tylko 15% odpowiedziało, że mają nad nimi pełną kontrolę. Jednocześnie sześciu na dziesięciu respondentów wskazało, że nie ufają firmom internetowym (63%) czy też firmom telefonicznym oraz internetowym dostawcom usług (62%). Respondenci mają również poważne obawy co do konsekwencji gromadzenia, przetwarzania i wykorzystywania ich danych. Siedem na dziesięć osób ma obawy co do wykorzystywania ich danych w celach innych niż ten, dla którego je pierwotnie zebrano.

Poniżej zidentyfikowano podstawowe zagrożenia dla skutecznej ochrony danych osobowych wynikające z rozwoju nowoczesnych technologii i wyzwania na najbliższe lata, przed jakimi stoi polski organu ochrony danych osobowych .

1. Profilowanie

Mechanizm profilowania Rada Europy w Rekomendacji CM/Rec (2010) 13 definiuje jako automatyczną technikę przetwarzania danych polegającą na przypisaniu danej osobie „profilu" w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw. Profilowanie oznacza kategoryzowanie osób według różnych cech (np. płci, wieku, pochodzenia etnicznego, wzrostu) lub zachowań (np. nałogów, codziennych rutyn, stylu życia, hobby) i wyciągnięcie na ich temat pewnych wniosków w oparciu o zebrane i przetworzone informacje. Profilowanie, jako automatyczna operacja na danych, obarczone jest ryzykiem błędu – w efekcie, w odniesieniu do danej osoby mogą

zostać przypisane założenia, które jej w rzeczywistości nie dotyczą. Do tego rodzaju operacji odnosi się art. 26a ust. 1 ustawy o ochronie danych osobowych, zgodnie z którym niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

Profilowanie ma szerokie spektrum zastosowań. Przedsiębiorcy na podstawie otrzymanych profili mogą dopasować nie tylko reklamy, ale też same produkty i usługi do potrzeb konkretnych osób. Z mechanizmu profilowania chętnie korzystają również banki i ubezpieczyciele, zatem na jego podstawie mogą być podejmowane ważne dla obywateli decyzje, np. o przyznaniu ubezpieczenia lub kredytu. Przykładowo, wiek kierowcy może być jedną z cech, od której uzależniona jest wysokość składek OC za samochód, a uzależnienie od papierosów – czynnikiem wpływającym na wysokość składki za ubezpieczenie zdrowotne.

Profilowanie jest także wykorzystywane przez sektor publiczny – Policję i inne organy bezpieczeństwa oraz administrację w celu prowadzenia polityki społecznej. To właśnie ten mechanizm jest podstawą wyodrębniania spośród pasażerów linii lotniczych osób, które potencjalnie mogą stwarzać zagrożenie dla bezpieczeństwa publicznego. W polskim systemie prawnym przez pryzmat mechanizmu profilowania oceniana jest możliwość otrzymania przez bezrobotnego konkretnej formy pomocy. Takie rozwiązanie jest wynikiem reformy urzędów pracy, która weszła w życie w maju 2014 r. Generalny Inspektor zwracał uwagę, że proces ten, będący poważną ingerencją w sferę prywatności i autonomii informacyjnej jednostki, wymaga odpowiednich gwarancji w przepisach powszechnie obowiązującego prawa, których w żadnej mierze nie zapewniają obecnie obowiązujące przepisy.

Reforma unijnego prawa ochrony danych osobowych daje szansę na „ucywilizowanie" procesu profilowania. Wprowadzone mają zostać ograniczenia dotyczące profilowania, które wywołuje skutki prawne lub ma istotny wpływ na osobę fizyczną, a oparte jest wyłącznie na automatycznym przetwarzaniu danych. Profilowanie ma być dopuszczalne jedynie w ściśle określonych sytuacjach: podczas zawierania lub wykonania umowy, na podstawie przepisów prawa lub po uzyskaniu zgody podmiotu danych. Ponadto, projekt przewiduje obowiązek poinformowania osoby, która podlega profilowaniu. Również art. 26a ust. 1 ustawy o ochronie danych osobowych zabrania dokonywania ostatecznych rozstrzygnięć indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

2. Biometria

Identyfikacja na podstawie danych biometrycznych bywa coraz częściej wykorzystywana np. w sektorze bankowym czy na potrzeby kontroli czasu pracy przez pracodawców. Metody biometryczne polegają na badaniu cech fizycznych (np. tęczówka oka, linie papilarne, kształt dłoni, układ żył w palcu czy nadgarstku, kształt małżowiny usznej, twarz, zapach), jak również cech związanych z zachowaniem (np. głos, sposób chodzenia, pisania na maszynie/klawiaturze, podpis odręczny). Dane biometryczne niewątpliwie można uznać za dane osobowe, jako pozwalające na ustalenie tożsamości określonej osoby w sposób pewny. Z racji ich wyłącznej przynależności do danej osoby, dane biometryczne stanowią pewnego rodzaju „identyfikator" człowieka. Dane te są niezmienne, co powoduje, że stanowią szczególny typ danych osobowych – dlatego do ich wykorzystywania należy podchodzić z dużą rozwagą, gdyż ich wyciek lub kradzież mogą mieć poważne w skutkach konsekwencje, nie tylko dla osób, których dane dotyczą.

Grupa Robocza art. 29[281] w dokumencie roboczym z 1 sierpnia 2003 r. dotyczącym biometrii wskazała, iż „(...) szybki rozwój technologii biometrycznych jak i coraz powszechniejsze ich stosowanie w ostatnich latach wymagają uważnej analizy z punktu widzenia ochrony danych. Powszechne i niekontrolowane posługiwanie się biometrią wzbudza niepokój z punktu widzenia ochrony wolności i fundamentalnych praw człowieka. (...) Szczególne zaniepokojenie związane z danymi biometrycznymi wzbudza ryzyko zmniejszenia wrażliwości ludzi spowodowane coraz większą powszechnością używania tych danych na konsekwencje, jakie przetwarzanie ich danych może mieć w ich życiu codziennym. (...) dane biometryczne zawsze mogą być uważane za „dane dotyczące osoby fizycznej", ponieważ dotyczy to danych ze swej natury dotyczących określonej osoby".

Metoda identyfikacji biometrycznej w oparciu o próbkę głosu miała zostać wdrożona w nowym Systemie Informacji Telefonicznej, przygotowywanym przez Ministerstwo Finansów. Generalny Inspektor krytykował to rozwiązanie, wskazując, że korzystanie z tego systemu nie tylko jest nadmierną ingerencją w prywatność człowieka, ale też nie jest niezbędne w realizacji ustawowych zadań fiskusa, zarówno w przypadku przetwarzania informacji o podatnikach, jak i informacji o urzędnikach. Ponadto, nie zostały stworzone

[281] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (Grupa Robocza Art. 29) powołana została na mocy art. 29 Dyrektywy 95/46/WE jako niezależny podmiot o charakterze doradczym. W skład Grupy Roboczej wchodzą przedstawiciele organu lub organów nadzorczych, powołanych przez każde Państwo Członkowskie, przedstawiciel organu lub organów ustanowionych dla instytucji i organów wspólnotowych oraz przedstawiciel Komisji.

stosowne przepisy, które mogłyby stanowić podstawę prawną dla funkcjonowania takiego systemu.

3. „Privacy by default", „privacy by design", „privacy impact assessment"

Koncepcja prywatności jako ustawienia domyślnego – *privacy by default* – oznacza, że ustawienia prywatności w urządzeniach, produktach lub usługach mają być nakierowane na maksymalną ochronę użytkownika i do niego ma należeć decyzja, czy i jakie dane chce udostępnić. Zgodnie z takim modelem administrator danych ma obowiązek zapewnić, by domyślnie przetwarzane były tylko te dane, które są niezbędne dla realizacji zakładanego celu. Konieczne jest również zapewnienie, że w tzw. opcji domyślnej dane osobowe nie będą udostępniane nieograniczonej liczbie osób. Obecnie domyślne ustawienia kreowane są przez dostawców usług w sposób swobodny, zatem najczęściej zakładają one udostępnianie danych w możliwie najszerszym zakresie (przykładowo – domyślne ustawienia wszystkich informacji jako „publiczne" na portalu społecznościowym). Przekształcenie dotychczasowego modelu zagwarantowałoby przestrzeganie podstawowych zasad ochrony danych, przede wszystkim zasady adekwatności, zgodnie z którą dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane.

Każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania - *privacy by design*. 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 wcześniej przewidywać najważniejsze z nich, analizując ryzyko wystąpienia określonych zdarzeń, czy dopuszczenia do zaniechań, i im przeciwdziałać.

Zasady *privacy by design* i *privacy by default* zostały zawarte również w przepisach ogólnego rozporządzenia o ochronie danych. Zgodnie z przepisami rozporządzenia, jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych (tzw. *privacy impact assessment*).

4. Prawo do bycia zapomnianym (*right to be forgotten*)

Prawo do bycia zapomnianym (prawo żądania usunięcia danych) daje osobie, której dane dotyczą, prawo – przy spełnieniu określonych warunków – do zaprzestania przetwarzania i usunięcia jego danych, zwłaszcza gdy brak jest uzasadnionego powodu do ich przechowywania. Rozwiązanie to nakłada na administratora danych obowiązek usunięcia danych określonej osoby, w przypadku otrzymania od niej odpowiedniego żądania, a następnie poinformowania osób trzecich również przetwarzających te dane, o tym żądaniu oraz usunięcia wszelkich linków lub kopii tych danych osobowych.

Idea prawa do bycia zapomnianym związana jest z faktem, iż w Internecie brak jest odpowiednika znanej z prawa karnego instytucji zatarcia skazania po upływie określonego czasu. „Wypowiedź, fotografia lub informacja o czynach staje się w Internecie nieusuwalna, wpływając jednocześnie przez lata, bez ograniczenia czasowego, np. na karierę zawodową lub polityczną osoby, której dotyczy" (M. Krzysztofek, *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy", 2012/8). Dlatego też tak ważne jest wyposażenie obywateli w mechanizm realnej, skutecznej kontroli nad dotyczącymi ich informacjami udostępnionymi w Internecie.

W dniu 13 maja 2014 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok sprawie Mario Costeja Gonzalez przeciwko Google Spain i Google Inc. (C-131/12). Orzeczenie to potwierdziło, iż operator wyszukiwarki internetowej w ramach swojej działalności nie tylko przetwarza dane osobowe, ale jest również ich administratorem, a zatem podmiotem, który decyduje o celach i środkach przetwarzania danych. Z tego powodu ciążą na nim określone obowiązki względem osób, których dane przetwarza. Na wniosek podmiotu danych operator wyszukiwarki zobowiązany jest do usunięcia konkretnego linku z listy wyników wyszukiwania, jeżeli życzy sobie tego dany podmiot. Jeśli nie podejmie on odpowiednich działań, podmiot danych może zwrócić się do właściwego organu z wnioskiem o nakazanie usunięcia linku.

Prawo do bycia zapomnianym pozwala na bardziej efektywną kontrolę nad danymi przez osoby, których one dotyczą. Koncepcja ta stanowi jeden z filarów reformy europejskiego prawa ochrony danych osobowych, jak również spore wyzwanie. Pojawiają się bowiem komentarze, że w praktyce realizacja tego prawa przez administratorów danych może okazać się zbyt skomplikowana.

5. Przetwarzanie danych telekomunikacyjnych przez Policję i służby

Problemy dotyczące okresu przechowywania (retencji) danych telekomunikacyjnych przez operatorów oraz granic inwigilacji obywateli przez służby od lat są przedmiotem zainteresowania Generalnego Inspektora Ochrony Danych Osobowych. Zasadniczą kwestią w tym zakresie jest określenie, jak szeroki ma być dostęp służb do danych retencyjnych (tj. jakie rodzaje danych są pozyskiwane, techniczne aspekty ich zbierania, czas przechowywania) oraz w jaki sposób mógłby on być kontrolowany. W tym kontekście kluczowe znaczenie mają dwa wydane w 2014 r. wyroki – Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości Unii Europejskiej.

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. akt K 23/11) za niezgodne z Konstytucją RP uznał przepisy ustaw o Policji i poszczególnych służbach w zakresie, w jakim nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych. Zakwestionowane przepisy mają stracić moc obowiązującą po upływie 18 miesięcy od ogłoszenia wyroku, tj. w lutym 2016 r.

W lipcu 2015 r. Senat RP przedstawił projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, który miał stanowić wykonanie wytycznych wynikających z wyżej wskazanego wyroku. Niestety, nie tylko w opinii GIODO zaproponowana nowelizacja nie stwarzała wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się obywateli, a tym samym nie stanowiła pełnej realizacji wyroku Trybunału. W toku prac legislacyjnych organ wskazywał na szereg elementów, które powinny się znaleźć w nowych przepisach, tj. wprowadzenie - jako zasady obowiązkowej - uprzedniej kontroli nad udostępnianiem danych telekomunikacyjnych, precyzyjne ograniczenie czasu przeprowadzania kontroli operacyjnej oraz przetwarzania danych telekomunikacyjnych, obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz o pozyskaniu informacji na jej temat, a także możliwość pozyskiwania informacji o jednostkach tylko w przypadku poważnych przestępstw.

Ponadto kwestia sięgania przez Policję i służby po dane telekomunikacyjne nie może zostać uregulowana w sposób prawidłowy bez odniesienia się do wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z dnia 8 kwietnia 2014 r. Stwierdzał on nieważność całego aktu prawnego, jakim jest dyrektywa 2006/24 w sprawie zatrzymywania danych w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland. Jako przyczynę nieważności dyrektywy 2006/24 w sprawie zatrzymywania danych, Trybunał wskazał brak

proporcjonalności zawartych w niej rozwiązań, które - mimo iż adekwatne do celu, który ma zostać za ich pomocą osiągnięty - ingerują zbyt głęboko w prawa podstawowe. TSUE uznał, że ten sam cel (zwalczanie poważnej przestępczości oraz zapewnienie bezpieczeństwa publicznego) można było osiągnąć środkami, które w mniejszym stopniu ingerują w prawa jednostek. Mimo, iż wyrok w sprawie Digital Rights Ireland nie powoduje automatycznie nieważności aktów prawa krajowego implementujących dyrektywę 2006/24, to konieczne jest uwzględnienie go w pracach legislacyjnych nad przepisami ustawy, które dotyczą tej samej materii.

6. Monitoring wizyjny

Jedną z najbardziej problematycznych i wymagających uregulowania w przepisach prawa kwestii, jest stosowanie monitoringu wizyjnego. W Polsce, podobnie jak w większości pozostałych państw europejskich, kamery monitoringu spotkać można na każdym kroku: na ulicach, w bankach, szkołach, szpitalach, obiektach sportowych czy sklepach. Z badań przeprowadzonych w 2012 r. przez Fundację Panoptykon we współpracy z Biurem Rzecznika Praw Obywatelskich, wynika, że kamery miejskie monitoringu wizyjnego zainstalowane są w 89 % polskich miast (miasta wojewódzkie i powiatowe), co już obrazuje skalę zjawiska.

Choć wideonadzór obecnie towarzyszy obywatelom niemal w każdej dziedzinie życia, wciąż nie został kompleksowo unormowany na poziomie ustawy dedykowanej tej kwestii. Istnieją jedynie szczątkowe regulacje dotyczące niektórych aspektów działania monitoringu, np. w ustawie o Policji czy ustawie o strażach gminnych. Ustawa o ochronie danych osobowych nie reguluje w sposób szczególny kwestii przetwarzania danych wizualnych i dźwiękowych (choć niewątpliwie tego rodzaju informacje stanowić mogą dane osobowe). Monitorowanie zachowań osób, uzasadniane najczęściej względami bezpieczeństwa, silnie ingeruje w prywatność i jako takie powinno doczekać się kompleksowej regulacji dotyczącej konkretnie tego zagadnienia. Bowiem do kwestii związanych z monitoringiem wizyjnym, ze względu na specyfikę tego zagadnienia, nie zawsze jest możliwe zastosowanie przepisów o ochronie danych osobowych. W 2011 r. Generalny Inspektor Ochrony Danych Osobowych skierował w tej sprawie sygnalizację do Ministra Spraw Wewnętrznych i Administracji wraz z opracowaniem *"Wymagania w zakresie regulacji monitoringu"*. Generalny Inspektor wyraził wówczas stanowisko, iż konieczne jest zainicjowanie prac legislacyjnych mających na celu unormowanie w przepisach rangi ustawowej ogólnych zasad i warunków

dopuszczalności stosowania monitoringu wizyjnego, celów, do jakich może być wykorzystywany, a także okresu przechowywania nagrań i ich ewentualnego publikowania.

Wskazać w tym miejscu należy na opinię nr 4/2004 Grupy Roboczej Art. 29, w której zwrócono uwagę m.in. na konieczność respektowania zasady proporcjonalności (adekwatności) przy posługiwaniu się wideonadzorem. Zasada ta oznacza, 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 lub bezpieczeństwa, niewymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami.

Istotne znaczenie ma w tej materii realizacja obowiązku informacyjnego wobec osób, których dane osobowe pozyskane zostały za pomocą monitoringu wizyjnego. Osoby te muszą mieć świadomość faktu prowadzenia wobec nich czynności wideonadzoru, tablice informacyjne o monitoringu wizyjnym powinny być widoczne i umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc.

Warto w tym miejscu wspomnieć także o wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie w sprawie o sygn. C-212/13 Ryneš z dnia 11 grudnia 2014 r. W wyroku tym Trybunał uznał, iż wykorzystywanie systemu kamer monitoringu wizyjnego zainstalowanego przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, jako monitorującego również przestrzeń publiczną, nie stanowi wyłącznie przetwarzania danych w celach osobistych i domowych – a zatem nie zajdzie w tym przypadku wyłączenie stosowania przepisów o ochronie danych osobowych. Co istotne, TSUE nie kwestionował, że obraz osoby zarejestrowany przez kamerę, o ile pozwala ustalić jej tożsamość, stanowi dane osobowe w rozumieniu przepisów dyrektywy 95/46/WE.

7. Przekazywanie danych do Stanów Zjednoczonych Ameryki

Wielkie firmy internetowe, z Facebookiem i Google włącznie, przetwarzają dane swoich użytkowników poza terenem Unii Europejskiej, co w praktyce negatywnie wpływa na interesy osób, których te dane dotyczą. Najbardziej jaskrawym przykładem są tu transfery danych do Stanów Zjednoczonych, bowiem już samo amerykańskie podejście do problematyki ochrony prywatności w znaczący sposób różni się od europejskiego. W przypadku USA mamy do czynienia z rozproszonymi przepisami o charakterze sektorowym –

brak jest regulacji o charakterze ogólnym, która wiązałaby wszystkie podmioty, zarówno publiczne, jak i prywatne.

Z uwagi na różnice pomiędzy prawodawstwem Unii Europejskiej oraz Stanów Zjednoczonych państwo to nie może zostać uznane za gwarantujące odpowiedni poziom ochrony danych osobowych. Sytuacja taka w znacznym stopniu hamuje wymianę gospodarczą pomiędzy Unią Europejską a Stanami Zjednoczonymi. Dlatego Departament Handlu Stanów Zjednoczonych - w porozumieniu z Komisją Europejską – w 2000 r. opracował program *Safe Harbour* („bezpieczna przystań") umożliwiający amerykańskim podmiotom gospodarczym sprostanie wymaganiom unijnej dyrektywy. Uzyskanie certyfikatu programu *Safe Harbour* przez uczestniczące w nim podmioty miało zapewnić, że gwarantują one odpowiedni poziom ochrony danych osobowych, o którym mowa w dyrektywie 95/46/WE.

Praktyka pokazała jednak wiele niedoskonałości związanych z funkcjonowaniem programu. Jak wykazały przeprowadzone przez Komisję Europejską analizy, nawet na podstawowym poziomie występowały problemy z przestrzeganiem jego zasad. Ponadto samo przekazanie danych do podmiotu legitymującego się certyfikatem *Safe Harbour* nie gwarantowało, że nie będą one wykorzystywane w inny sposób, np. przez organy ścigania.

W dniu 6 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej wydał przełomowy wyrok w sprawie Maximilian Schrems vs Data Protection Commissioner (C-362-14), w którym stwierdził nieważność decyzji Komisji Europejskiej w sprawie adekwatności zasad ochrony prywatności przewidzianych w ramach „bezpiecznej przystani" przez Stany Zjednoczone. To rozstrzygnięcie powoduje, że konieczne jest wypracowanie nowych, politycznych, prawnych i technicznych rozwiązań umożliwiających przekazywanie danych na terytorium Stanów Zjednoczonych z poszanowaniem praw podstawowych. Skuteczne pozostają jednak wszystkie pozostałe przesłanki legalizujące transfer danych osobowych. Nadal mogą być więc wykorzystywane standardowe klauzule umowne i Wiążące Reguły Korporacyjne, aczkolwiek problematyczna w indywidualnych przypadkach pozostaje kwestia, czy przesłanki te są w istocie stosowane w miejsce zasad wynikających z programu *Safe Harbour*, zakwestionowanych przez Trybunał.

8. Kradzież tożsamości

Z przypadkiem kradzieży tożsamości możemy mieć do czynienia, gdy ktoś np. podszywając się pod inną osobę dokona transakcji jej kartą płatniczą lub zaciągnie na jej

nazwisko kredyt w banku. Źródła i sposoby pozyskiwania informacji o osobach mogą być bardzo różne, od kradzieży po wyłudzenie. poprzez podszywanie się pod jakąś instytucję czy osobę. Przestępstwo kradzieży tożsamości ostatnio popełniane jest na niespotykaną dotąd skalę. To właśnie jeden ze skutków żywiołowego rozwoju nowych technologii. Arkadiusz Lach, powołując się na źródła angielskie, wskazuje, że „(…) przywłaszczenie cudzej tożsamości jest określane przestępstwem Nowego Milenium, czyli przestępstwem Wieku Informacji" (*Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Wolters Kluwer, Warszawa 2015).

W polskim prawie karnym niezbędną przesłanką dla uznania kradzieży tożsamości za działanie bezprawne jest wyrządzenie szkody osobistej lub materialnej poprzez wykorzystanie danych innej osoby. Stanowi o tym wprost art. 190a § 2 Kodeksu karnego.

Zjawisko popełniania przestępstw związanych z kradzieżą tożsamości ma charakter niezwykle dynamiczny i stal rośnie, powodując wymierne straty. Według Raportu Komisji Europejskiej z 2015 r. zjawiskiem tym dotkniętych zostało około 2% mieszkańców UE, a średnia szkoda to 2500 euro. W Polsce, według badań przeprowadzonych przez TNS OBOP w 2008 r. jedynie 7% respondentów wskazało, iż padło ofiarą kradzieży tożsamości, podczas gdy w roku 2013 było to już 17%. Co istotne, aż 46% ofiar zadeklarowało, że konsekwencją bezprawnego wykorzystania ich danych osobowych była kradzież z ich rachunków bankowych.

Niezwykle istotnym elementem walki z tą przestępczością jest wzmożenie edukacji w zakresie prawa i zasad ochrony danych, w celu podnoszenia świadomości i wiedzy zarówno osób, których dane dotyczą, jak i podmiotów przetwarzających dane. Oprócz działalności edukacyjnej powinno się zainicjować stworzenie krajowej strategii ochrony przed tym coraz powszechniejszym zjawiskiem. W wielu państwach, m.in. w Australii, wprowadzono wydawanie certyfikatów dla pokrzywdzonych kradzieżą tożsamości po prawomocnym skazaniu sprawcy. Dzięki temu osoby, którym skradziono tożsamość, nie musiałyby składać wyjaśnień we wszystkich postępowaniach prowadzonych przez policję czy sąd w miarę wykrywania kolejnych przestępstw dokonywanych przez osobę, która dokonała kradzieży danych. Wystarczyłoby bowiem jednorazowe oczyszczenie ich z zarzutu i odnotowanie tego np. w specjalnym rejestrze. Uchroniłoby to osoby poszkodowane przed czasochłonnymi i kosztownymi – często poza miejscem ich zamieszkania – wizytami na policji czy w sądzie, a także usprawniło pracę wymiaru sprawiedliwości.

9. Internet Rzeczy

Internet Rzeczy, inaczej Internet Przedmiotów (*Internet of Things*) to koncepcja, wedle której przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem sieci komputerowej. Do tego typu przedmiotów zaliczają się między innymi urządzenia grzewcze, gospodarstwa domowego, liczniki wody czy energii elektrycznej, ale również samochody, ubrania, a nawet artykuły spożywcze. Na rynku dostępne są też ponadto inteligentne urządzenia noszone na ciele lub w ciele człowieka – zliczające przebiegnięte kilometry, ale także mierzące poziom cukru czy monitorujące funkcjonowanie organizmu osoby chorej.

Z Internetem Rzeczy powiązana jest również idea „inteligentnego miasta" (*Smart City*), czyli miasta wykorzystującego rozwiązania teleinformatyczne dla lepszego funkcjonowania i zarządzania infrastrukturą miejską. Zastosowanie rozwiązań *Smart City* wiąże się również z gromadzeniem informacji, w tym danych osobowych, na temat mieszkańców i innych osób znajdujących się na terenie miasta.

Jak zwracała uwagę Grupa Robocza Art. 29 podczas prac nad opinią w sprawie Internetu Przedmiotów, większość inteligentnych urządzeń nie jest projektowana z myślą o interoperacyjności, ale w celu przesyłania danych bezpośrednio do producenta urządzenia, który następnie staje się administratorem danych. Użytkownicy mogą uzyskać dostęp do swoich danych w sieci lub przy użyciu aplikacji w smartfonach, ale nie mogą zapobiec przekazywaniu danych do administratora danych. Podczas gdy istniejące urządzenia mierzą dane typowe dla środowiska, nowe urządzenia skupiają się bardziej na obserwacji zwyczajów użytkowników, zatem mogą obejmować przetwarzanie danych osobowych.

Choć wskazane wyżej koncepcje mogą przynieść różnego rodzaju ułatwienia w codziennym życiu – od drobnych udogodnień po ratowanie życia – wiążą się z nimi również potencjalne zagrożenia dla prywatności. Rozwój technologiczny nie powinien być hamowany, zwłaszcza jeśli w założeniu ma się wiązać z pewnymi korzyściami dla jednostek i poprawą jakości jej życia. Ale jednocześnie nie może odbywać się kosztem ochrony danych osobowych – konieczne jest zatem odpowiednie wyważenie wartości i zachowanie maksimum prywatności, nie umniejszając jednocześnie pozytywnych aspektów inteligentnych technologii.

Poniżej opisane zostaną – przykładowo – dwa wybrane zagadnienia związane z koncepcją „Internetu Rzeczy", a mianowicie inteligentne liczniki energii elektrycznej oraz technologia RFID.

9.1. Inteligentne liczniki energii – *smard grid*

Podstawowy model systemów energetycznych przechodzi w ostatnich latach głęboką przemianę. Dzięki technologii teleinformatycznej przeistoczył się ze względnie prostego układu dostawca - odbiorca, w układ zbliżony do rozproszonej sieci komputerowej o wielostronnym przepływie energii i informacji.

W założeniu zintegrowany system zbierania informacji o zużyciu prądu ma umożliwić bardziej świadome zarządzenie energią elektryczną. Z jednej strony dostawca będzie dokładnie wiedział, ile prądu potrzebujemy i dzięki temu będzie mógł ograniczać straty związane z przesyłem, które są istotne w globalnym wymiarze tego zjawiska. System zakłada także wprowadzenie zróżnicowanych taryf w zależności od tego, kiedy korzystamy z energii.

Z drugiej jednak strony, przy pomocy danych zebranych przez inteligentne liczniki i dokonanej na ich podstawie analizy schematów zachowań, można w łatwy sposób opracować profil osobowy użytkowników zamieszkałych pod danym adresem. W oparciu o wskazania licznika można ocenić, czy np. ktoś jest w domu, jakie ma zwyczaje, jakich urządzeń używa. Dlatego trzeba sobie jasno zdawać sprawę, że zarówno na etapie tworzenia prawa dla tych systemów, jak i stosowania ich w praktyce, kwestie związane z ochroną prywatności powinny stanowić priorytet i być przedmiotem wnikliwej analizy celem przyjęcia rozwiązań jak najmniej ingerujących w autonomię informacyjną i prywatność jednostek. Konieczne jest przykładowo ustalenie częstotliwości przesyłu danych, uzależnienie zakresu przekazywanych danych od celu, w jakim będą wykorzystywane oraz określenie czasu, przez który dane mają być przechowywane.

9.2. Technologia RFID

Technologia identyfikacji radiowej (ang. *Radio Frequency Identification* – RFID) umożliwia automatyczną identyfikację obiektów. Jej zastosowanie polega na wykorzystaniu miniaturowych urządzeń zwanych znacznikami lub tagami RFID. Wyposaża się w nie coraz więcej przedmiotów, m.in. towary w sklepach. Dzięki zainstalowaniu takich mikroprocesorów, które mogą być odczytywane bezprzewodowo za pomocą fal radiowych, możliwe jest pozyskiwanie wiedzy zarówno na temat wyposażonych w nie przedmiotów, jak i osób, które je użytkują. Najczęściej odbywa się nie tylko bez naszej zgody, ale i wiedzy, co rodzi zagrożenia dla naszej prywatności.

Systemy RFID są obecnie powszechnie wykorzystywane m.in. do zabezpieczania towarów przed kradzieżami. Ponadto technologia ta pozwala na gromadzenie rozmaitych

danych dotyczących określonej osoby, śledzenie obywateli poruszających się po miejscach publicznych, takich jak np. lotniska, centra handlowe, dworce czy ulice. Jej zastosowanie daje możliwość wzbogacania profili poprzez monitorowanie zachowań konsumentów w sklepach, odczytywania informacji m.in. o noszonych ubraniach i używanych akcesoriach.

Zwolennicy tych rozwiązań podnoszą liczne zalety tej technologii, akcentując przede wszystkim kwestie bezpieczeństwa. Obawy jednak wzbudza możliwość zdalnej identyfikacji lub uzyskania dostępu do informacji przez osoby do tego nieupoważnione.

Według przyjętych przez Komisję Europejską zaleceń, państwa członkowskie powinny zagwarantować skuteczne mechanizmy ochrony danych osobowych przetwarzanych przy wykorzystaniu technologii RFID. W szczególności przedstawiciele sektora handlu detalicznego zobowiązani zostali do informowania osób fizycznych - poprzez stosowanie wspólnego znaku europejskiego - o identyfikatorach umieszczonych lub wbudowanych w produkty. Przy sprzedaży identyfikatory te powinny być dezaktywowane lub usuwane, chyba że konsumenci wyrażą zgodę na dalsze ich działanie.

Konieczna jest również lepsza edukacja osób, których stosowanie technologii RFID może dotyczyć.

10. Centralne zbiory danych osobowych

W związku z dynamicznym rozwojem technologii i informatyzacją administracji publicznej, coraz częściej tworzone są różnego rodzaju państwowe rejestry, dzięki którym liczne podmioty w szerokim zakresie mogą przetwarzać informacje o obywatelach.

Tego typu centralne systemy stworzone zostały w sektorze szkolnictwa (System Informacji Oświatowej) oraz w sektorze ochrony zdrowia (System Informacji Medycznej). W państwowych rejestrach przetwarzane są również m.in. dane osób bezrobotnych czy korzystających z pomocy społecznej. Wskazać można ponadto na prowadzoną przez Ministerstwo Sprawiedliwości elektroniczną Centralną Bazę Danych Ksiąg Wieczystych.

Konstruowanie wielkich publicznych baz danych nie może odbywać się bez uwzględnienia wpływu tworzonego systemu na prywatność osób fizycznych i z pominięciem zasad wynikających z przepisów Konstytucji RP, ustawy o ochronie danych osobowych i wydanych na jej podstawie rozporządzeń wykonawczych. Każdorazowo takie działania muszą mieć miejsce z uwzględnieniem koncepcji *privacy by default, privacy by design* oraz *privacy impact assessment",* opisanych w punkcie 3. Istotne jest, by to w przepisach rangi ustawy regulowane były zasadnicze kwestie związane z funkcjonowaniem rejestru, a

mianowicie katalog przetwarzanych danych, okres ich przechowywania, zasady udostępniania informacji z rejestru, czy też krąg podmiotów mających dostęp do danych. Zasada prymatu przepisów ustawowych wynika również ze stanowisk Trybunału Konstytucyjnego, m.in. w postanowieniu z dnia 31 stycznia 2007 r. (sygnatura S 1/2007), Trybunał wskazał, iż „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". Wymóg umieszczenia bezpośrednio w ustawie wszystkich zasadniczych elementów regulacji prawnej musi być stosowany ze szczególnym rygoryzmem, gdy regulacja ta dotyczy korzystania przez obywateli z ich praw i wolności (wyrok Trybunału Konstytucyjnego z dnia 25 maja 1998 r. sygnatura U 19/97). Podobnie orzekł Trybunał w wyroku z dnia 18 grudnia 2014 r. (sygnatura K 33/13), dotyczącym tworzenia rejestrów danych medycznych na podstawie rozporządzenia przez Ministra Zdrowia.

Dopiero sformułowanie właściwych zasad w przepisach ustawy (dedykowanej danemu zagadnieniu czy sektorowi albo działowi administracji) stwarza podstawy do funkcjonowania danego rejestru. W praktyce często jednak okazuje się, że w pierwszej kolejności dokonywany jest zakup systemu informatycznego, do którego następnie dopasowywane są tworzone regulacje prawne. Niejednokrotnie u podstaw tworzenia rejestrów znajdują się akty niższego rzędu niż ustawa bądź też regulacje pozaustawowe (porozumienia, umowy, wytyczne, itp.), co jest niezgodne z konstytucyjną zasadą legalizmu (art. 51 Konstytucji RP).

Pojawiają się także wątpliwości związane z dopuszczalnością przekazywania danych osobowych między różnymi rejestrami. Bywa, że do dokonywania takich operacji – w miejsce tworzenia właściwych przepisów prawa w tym zakresie – wykorzystywana jest instytucja powierzenia przetwarzania danych osobowych uregulowana w art. 31 ustawy o ochronie danych osobowych, co jest niezgodne z obowiązującym prawem. Należy bowiem podkreślić, że 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 własnych celów lub interesów tegoż podmiotu. Administrator nie może powierzyć innemu podmiotowi przetwarzania danych w celu innym, niż ten, dla którego on je przetwarza. Doprowadziłoby to bowiem do sytuacji, w której administrator przeniósłby na inny podmiot

uprawnienia, których sam nie posiada. Nie może także dochodzić mocą umowy cywilno-prawnej do cedowania uprawnień poszczególnych organów czy regulowania mocą umowy kwestii podstawowych, jakimi są zasady przetwarzania danych osobowych, które regulować mogą jedynie przepisy powszechnie obowiązującego prawa, zwłaszcza w przypadku przetwarzania danych szczególnie chronionych. Stosowaną na poziomie centralnym praktyką, niedopuszczalną z punktu widzenia ochrony danych osobowych, jest kopiowanie istniejących zbiorów, by mógł z nich skorzystać inny podmiot, zamiast czerpania z dostępnych rozwiązań wynikających z obowiązujących przepisów prawa określających zasady dostępu do informacji zawartych w danym zbiorze.

Z tychże względów tworzenie rejestrów zawierających dane osobowe musi być poprzedzone dokładną analizą wpływu projektowanych rozwiązań na ochronę danych, co jest szczególnie ważne zwłaszcza w przypadku centralnych zbiorów danych administrowanych przez podmioty publiczne, które mają obowiązek działać na podstawie i w granicach przepisów powszechnie obowiązującego prawa, kompleksowo regulujących istnienie tychże zbiorów i zasady przetwarzania informacji o osobach (m.in. wskazujących warunki zasilania centralnych baz, czerpania z ich zasobów, czy też retencji danych w nich zawartych).

Podkreślić należy, iż GIODO będzie zwracał szczególną uwagę na kwestie związane z funkcjonowaniem istniejących, a także dopiero projektowanych rejestrów o charakterze centralnym. Związana z tym będzie analiza zasadności gromadzenia danych na poziomie centralnym, bowiem nie w każdym przypadku konieczny jest taki dostęp do szerokiego katalogu informacji o osobie. Tam, gdzie to możliwe, powinien być zaproponowany inny model realizacji określonych zadań – tak, aby przetwarzanie określonych danych osobowych na poziomie centralnym miało miejsce wyłącznie wtedy, gdy jest rzeczywiście niezbędne z uwagi na wskazany w przepisach prawa cel.

11. Ponowne wykorzystanie informacji publicznej

Udostępnienie informacji znajdujących się w zasobach administracji publicznej do powtórnego wykorzystania, rodzi pewne obawy związane z ochroną naszych danych. Dotyczą one przede wszystkim sytuacji, w której dochodzić może do nieuprawnionego łączenie danych osobowych, które pochodzą z różnych zbiorów będących w posiadaniu administracji publicznej.

Zgodnie z przepisami prawa Unii Europejskiej, co do zasady obecnie obowiązkowe jest, aby organy sektora publicznego pozwalały na ponowne wykorzystywanie wszystkich

informacji, które posiadają, zarówno do celów komercyjnych, jak i niekomercyjnych. Powyższe wynika to z dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, nazywanej również dyrektywą reuse.

Jak wskazała Grupa Robocza Art. 29 w opinii 06/2013, ponowne wykorzystywanie informacji sektora publicznego może przynieść korzyści społeczeństwu, w tym większą przejrzystość sektora publicznego oraz przyczynienie się do innowacyjności. Niemniej jednak zwiększenie dostępności informacji publicznych, szczególnie gdy obejmują one dane osobowe, nie pozostaje bez wiążących się z tym zagrożeń. Dlatego też istotne jest posiadanie solidnej podstawy prawnej do publicznego udostępniania danych osobowych, z uwzględnieniem istotnych zasad ochrony danych, w tym zasad proporcjonalności, ograniczenia celu oraz minimalizacji zakresu danych. W celu zapewnienia odpowiednich zabezpieczeń zaleca się przeprowadzenie oceny wpływu na ochronę danych, zanim informacje sektora publicznego obejmujące dane osobowe, zostaną udostępnione do ponownego wykorzystania.

Przepisy dotyczące ponownego wykorzystania informacji publicznej w praktyce umożliwiają podmiotom spoza sektora administracji publicznej łączenie danych pochodzących z jawnych rejestrów, które do tej pory były prowadzone wyłącznie przez władzę publiczną. Pewien niepokój budzi w tym kontekście brak rozróżnienia w polskim prawie pomiędzy jawnością formalną danych, które mogą stanowić informacje publiczną a tak zwaną „otwartością", która nie jest w polskim prawie zdefiniowana. Brak definicji otwartości prowadzić może do traktowania informacji jawnej formalnie jako informacji możliwej do dowolnego przetwarzania.

Jako przykład posłużyć mogą tu dane z elektronicznych ksiąg wieczystych oraz dane z Krajowego Rejestru Sądowego, zawierające np. informacje o numerze PESEL poszczególnych osób fizycznych. Jeżeli połączymy je z danymi z innych rejestrów, np. z powszechnie dostępnego rejestru pośredników w handlu nieruchomościami zawierającego dane o imieniu, nazwisku i miejscu zamieszkania pośrednika, to otrzymamy wyraźny profil konkretnej osoby. Informacja przekazana do ponownego wykorzystania może służyć do profilowania osoby fizycznej i wyciągania z kształtu takiego profilu wniosków, które mogą następnie prowadzić np. do dyskryminacji osoby.

Przy łączeniu w nowych zbiorach danych pochodzących z publicznych rejestrów nadal konieczne jest przestrzeganie zasad ochrony danych osobowych, czego nie zawsze są

świadomi przetwarzający takie dane osobowe, przede wszystkim wypełnienie obowiązku informacyjnego wobec osób, których dane dotyczą. Brak informacji co do źródeł pozyskania danych o osobie i o celach, w jakich są udostępniane uniemożliwia skorzystanie z prawa żądania usunięcia danych czy też złożenia sprzeciwu wobec ich przetwarzania.

12. Big Data

Big Data (duże zbiory danych, gigadane) to gigantyczne zbiory danych cyfrowych będące w posiadaniu przedsiębiorstw, rządów i innych dużych organizacji. Zbiory te poddawane są szczegółowej analizie przy użyciu algorytmów komputerowych. Uznaje się, że możliwość przechowywania i analizowania ogromnych ilości danych może być przydatna dla społeczeństwa. Big Data mogą być bowiem wykorzystywane na przykład do przewidywania rozpowszechniania się epidemii, wykrywania poważnych skutków ubocznych lekarstw oraz zwalczania zanieczyszczenia środowiska w dużych miastach. Niektóre z tych zastosowań z pozoru nie wiążą się z danymi osobowymi. Jednakże Big Data mogą być również wykorzystywane w sposoby budzące istotne obawy, co do ochrony prywatności osób i praw obywatelskich, ochrony przed dyskryminacyjnymi skutkami oraz naruszeniami prawa do równego traktowania.

Analityka biznesowa danych nie jest sama w sobie zakazana. Trzeba jednak pamiętać, że gdy dotyczy danych objętych ochroną, zarówno przez prawo ochrony danych osobowych, jak i w związku z istnieniem tajemnic prawnie chronionych, jak np. tajemnica bankowa lub telekomunikacyjna – posiadacze takich danych nie mogą się nimi swobodnie dzielić. Nie można także ich łączyć. Prawo zabrania zestawiania danych pozyskanych na różne potrzeby bez zgody osób, których one dotyczą lub bez innej wyraźnej podstawy prawnej. Zgoda ta musi być świadoma, niewymuszona, poprzedzona obowiązkiem informacyjnym. Tymczasem często obserwuje się działania podmiotów biznesowych polegające na umiejętnym ukrywaniu informacji mających na celu podanie rzeczywistego celu ich pozyskiwania od osób zainteresowanych.

Niepokojącą kwestią jest również analityka predykcyjna, w której z cech, uważanych za prawdziwe albo uprawdopodobnione, próbujemy wnioskować o cechach, które jeszcze uprawdopodobnione nie są. Takie działanie jest dopuszczalne wyłącznie w sytuacji, gdy wymaga tego prawo albo w sytuacji, gdy istnieje zgoda ze strony osoby zainteresowanej. Musi być ona jednak poinformowana, że takie działania są podejmowane, na

czym polegają oraz zawsze powinna mieć dostęp do informacji o tym, jakie dane na jej temat zostały zebrane i w jaki sposób są przetwarzane.

Powyższe kwestie należy uznać za jedne z tych, które w ocenie Generalnego Inspektora Ochrony Danych Osobowych uważane są za znaczące, jeśli chodzi o wyzwania związane z zapewnieniem ochrony danych osobowych. Ze względu na ich znaczenie – zarówno w odniesieniu do sposobu funkcjonowania instytucji publicznych, jak i podmiotów komercyjnych – winny być one przedmiotem zainteresowania organu stojącego na straży zasad ochrony danych osobowych.

ZAŁĄCZNIKI:

Załącznik nr 1

Wykaz najważniejszych wystąpień Generalnego Inspektora Ochrony Danych Osobowych w roku 2015 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.	Urząd Miejski w Jarocinie	17.04.2015 DOLiS-035-451/15	Wystąpienie z art. 19a ust. 1 ustawy o ochronie danych osobowych skierowane do Urzędu Miejskiego w Jarocinie w związku z pozyskiwaniem szerokiego zakresu danych osobowych od osób odwiedzających miejskie muzeum.
2.	Urząd Gminy Dywity	17.04.2015 DOLiS-035-750/15	Wystąpienie z art. 19a ust. 1 ustawy skierowane do Urzędu Gminy Dywity dotyczące pozyskiwania szerokiego zakresu danych osobowych od mieszkańców gminy wypełniających na stronie urzędu ankietę dotyczącą planu gospodarki niskoemisyjnej.
3.	Urząd Miejski Kalisz	13.04.2015 DOLiS-035-756/15	Wystąpienie z art. 19a ust. 1 ustawy skierowane do Urzędu Miejskiego w Kaliszu w związku z nieprawidłowym przechowywaniem korespondencji skierowanej do petentów urzędu.
4.	Kancelaria Prezesa Rady Ministrów	26.03.2015 DOLiS-035-1082/15	Wystąpienie z art. 19a ust. 1 ustawy skierowane do Prezesa Rady Ministrów z wnioskiem o wprowadzenie zmian w ustawie Prawo zamówień publicznych w zakresie regulacji dotyczących przetwarzania danych osobowych
5.	Ministerstwo Środowiska	02.03.2015 DOLiS-035-710/15	Wystąpienie z art. 19a ust. 1 ustawy skierowane do Ministerstwa Środowiska dotyczące treści deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi.
6.	Ministerstwo Edukacji Narodowej	02.03.2015 DOLiS-035-711/15	Wystąpienie z art. 19a ust. 1 ustawy do Ministerstwa Edukacji Narodowej w sprawie umieszczania numeru PESEL na drukach legitymacji szkolnych.
7.	Ministerstwo Infrastruktury i Rozwoju	02.03.2015 DOLiS-035-712/15	Wystąpienie z art. 19a ust. 1 ustawy do Ministerstwa Infrastruktury i Rozwoju dotyczące przetwarzania danych osobowych osób ubiegających się o najem lokali należących do mieszkaniowego zasobu gminy.
8.	Urząd Miasta Legnica	09.02.2015	Wystąpienie z art. 19a ust. 1 ustawy do Urzędu Miasta w Legnicy w związku z udostępnieniem

		DOLiS-035-751/14	danych osobowych osoby fizycznej (w tym również danych szczególnie chronionych) w odpowiedzi na wniosek o udostępnienie informacji publicznej.
9.	Zakład Karny w Iławie	28.09.2015 DOLiS-035-123/15	Wystąpienie z art. 19a ust. 1 ustawy do Zakładu Karnego w Iławie w związku z bezpodstawnym pozyskiwaniem szerokiego zakresu danych osobowych poprzez pozyskiwanie i archiwizowanie kopii dowodów tożsamości osób odwiedzających osadzonych.
10.	Ministerstwo Spraw Wewnętrznych	28.07.2015 DOLiS-035-2499/15	Wystąpienie z art. 19a ust. 1 ustawy do Ministerstwa Spraw Wewnętrznych z wnioskiem o podniesienie wśród wojewodów problemu niezgodnego z przepisami prawa przetwarzania (pozyskiwania) danych osobowych przez straże miejskie.
11.	Ministerstwo Spraw Wewnętrznych	28.07.2015 DOLiS-035-2498/15	Wystąpienie z art. 19a ust. 1 ustawy do Ministerstwa Spraw Wewnętrznych w sprawie podjęcia działań legislacyjnych mających na celu zapewnienie strażom gminnym dostęp do danych objętych tajemnicą telekomunikacyjną w zakresie, w jakim jest to niezbędne do przeprowadzenia czynności wyjaśniających.
12.	Wojewódzka Komisja Lekarska Mazowiecki Urząd Wojewódzki	20.05.2015 DOLiS-035-751/15	Wystąpienie na podstawie art. 19a ust. 1 ustawy w związku z uzyskaniem przez GIODO informacji, iż podczas kwalifikacji wojskowej dokonywanej przez komisję lekarską dane osobowe, w tym dane szczególnie chronione osób poddanych przedmiotowej kwalifikacji przetwarzane są w sposób umożliwiający zapoznanie się z nimi osobom do tego nieuprawnionym.
13.	Urząd Ochrony Konkurencji i Konsumentów	09.03.2015 DOLiS-035-538/15	Wystąpienie z art. 19a ust. 1 ustawy do Urzędu Ochrony Konkurencji i Konsumentów w związku z ujawnieniem kilkuset adresów mailowych osób, które komunikowały się z nim w sprawie kredytów frankowych.
14.	Urząd Miejski w Jarocinie	04.11.2015 DOLiS-035-555/15	Wystąpienie z art. 19a ust. 1 ustawy do Urzędu Miejskiego w Jarocinie w sprawie rozsyłania korespondencji w formie obejmującej rozdzielnik zawierający dane osobowe w postaci imion i nazwisk oraz adresów osób fizycznych.
15.	Urząd Miejski w Środzie Śląskiej	18.05.2015 DOLiS-035-4294/13	Wystąpienie z art. 19a ust. 1 ustawy do Urzędu Miejskiego w Środzie Śląskiej w związku z zamieszczeniem w Biuletynie Informacji Publicznej niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy, zawierających dane osobowe pracowników kontrolowanego urzędu.
16.	Urząd Skarbowy Wrocław-Fabryczna	18.05.2015 DOLiS-035-4294/13	Wystąpienie z art. 19a ust. 1 ustawy, do Urzędu Skarbowego Wrocław-Fabryczna w związku

			z zamieszczeniem w Biuletynie Informacji Publicznej niezanonimizowanych protokołów kontroli przeprowadzonych przez inspektorów pracy, zawierających dane osobowe pracowników kontrolowanego urzędu.
17.	Urząd Gminy w Osieku	21.08.2015 DOLiS-035-2203/15	Wystąpienie z art. 19a ust. 1 ustawy, do Urzędu Gminy w Osieku w związku z pozyskaniem przez GIODO informacji, iż podczas przeprowadzania czynności urzędowych przez pracowników urzędu gminy dochodzi do przetwarzania danych osobowych w sposób umożliwiający zapoznanie się z nimi osobom do tego nieuprawnionym.
18.	Minister Spraw Wewnętrznych	15.04.2015 DOLiS-035-1361/15	Wystąpienie z art. 19a ust. 2 ustawy, do Pani Teresy Piotrowskiej – ówczesnej Minister Spraw Wewnętrznych o podjęcie prac legislacyjnych mających na celu uregulowanie w przepisach rangi ustawowej zagadnienia Krajowego Systemu Informacyjnego Policji.
19.	Marszałek Sejmu	14.07.2015 DOLiS-035-2342/15	Wystąpienie z art. 19a ust. 2 ustawy, do Pani Małgorzaty Kidawy-Błońskiej – ówczesnej Marszałek Sejmu - o zainicjowanie w Sejmie Rzeczypospolitej Polskiej prac ustawodawczych zmierzających do znowelizowania art. 71 ustawy z dnia 18 grudnia 1998 roku o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu w celu zapewnienia jego zgodności z przepisami o ochronie danych osobowych.

Załącznik nr 2

Wykaz kontroli przeprowadzonych w 2015 r.

L.p.	Data / Sygnatura kontroli	Nazwa podmiotu i miejsce kontroli	Inicjatywa kontroli	Rozstrzygnięcie
1.	12-16.01.2015 DIS-K-421/1/15	Fundusz Hipoteczny Dom S.A., Warszawa, Al. Jana Pawła II 29	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
2.	12-16.01.2015 DIS-K-421/2/15	Fundusz Hipoteczny Dom S.A. s.k.a., Warszawa, Al. Jana Pawła II 29	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
3.	12-16.01.2015 DIS-K-421/3/15	Grupa Etendard Sp. z o.o. Warszawa, ul. Domaniewska 39	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
4.	12-13.01.2015 DIS-K-421/4/15	Grupa Wirtualna Polska Sp. z o.o. Warszawa, ul. Jutrzenki 137A	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
5.	19-22.01.2015 DIS-K-421/5/15	Warszawskie Zakłady Farmaceutyczne Polfa S.A. Warszawa, ul. Karolkowa 22/24	z urzędu	nie stwierdzono uchybień
6.	26-29.01.2015 DIS-K-421/6/15	Gremax Sp. z o.o. Kraków, Os. Złotej Jesieni 6/71	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
7.	26-27.01.2015 DIS-K-421/7/15	Teva Pharmaceuticals Polska Sp. z o.o., Warszawa, ul. Emilii Plater 53	z urzędu	nie stwierdzono uchybień
8.	02-06.02.2015 DIS-K-421/8/15	Toyota Logistics Services Poland Sp. z o.o. Warszawa, ul. Poleczki 23	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
9.	02-06.02.2015 DIS-K-421/9/15	Anixe Polska Sp. z o.o. Warszawa, ul. Grabiszyńska 241A	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
10.	02-06.02.2015 DIS-K-421/10/15	Top Secret Sp. z o.o. Łódź, ul. Żniwna 10/14	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
11.	02-06.02.2015 DIS-K-421/11/15	Benefit Systems S.A. Warszawa, ul. Fredry 6	w związku z kontrolą DIS-K-421/135/14	decyzja GIODO
12.	05-06.02.2015 DIS-K-421/12/15	Testa Communications Sp. z o.o. Warszawa, ul. Poniatowskiego 1	z urzędu	nie stwierdzono uchybień
13.	05-06.02.2015 DIS-K-421/13/15	Satoria Group S.A. Warszawa, ul. Ciołka 12	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
14.	09-13.02.2015 DIS-K-421/14/15	Ministerstwo Zdrowia, Warszawa, ul. Miodowa 15	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
15.	09-13.02.2015 DIS-K-421/15/15	PGNiG Termika S.A. Warszawa, ul. Modlińska 15	z urzędu	decyzja GIODO

16.	16-20.02.2015 DIS-K-421/16/15	Unizeto Technologies S.A. Szczecin, ul. Królowej Korony Polskiej 21	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
17.	16-20.02.2015 DIS-K-421/17/15	Kolej Gondolowa Jaworzyna Krynicka S.A. Krynica – Zdrój, ul. Czarny Potok 75	z urzędu	nie stwierdzono uchybień
18.	17-19.02.2015 DIS-K-421/18/15	Opus Finance Sp. z o.o. Warszawa, ul. Zielna 37	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
19.	18-20.02.2015 DIS-K-421/19/15	Stołeczne Centrum Sportu Aktywnego Warszawa, Warszawa, ul. Rozbrat 26	z urzędu	nie stwierdzono uchybień
20.	23-27.02.2015 DIS-K-421/20/15	Philipiak Polska S.A. sp. k. Warszawa, ul. Strażacka 63/65	z urzędu	w toku
21.	24-25.02.2015 DIS-K-421/21/15	Tomasz Jędrzejewski i Witold Jędrzejewski Piruet s.c. Warszawa, ul. Żabińskiego 9/26	z urzędu	nie stwierdzono uchybień
22.	25-27.02.2015 DIS-K-421/22/15	Ośrodek Sportu i Rekreacji m.st. Warszawy w Dzielnicy Targówek, Warszawa, ul. Łabiszyńska 20	z urzędu	nie stwierdzono uchybień
23.	25-27.02.2015 DIS-K-421/23/15	Miejski Ośrodek Sportu i Rekreacji Bystrzyca w Lublinie Sp. z o.o. Lublin, ul. Filaretów 44	z urzędu	nie stwierdzono uchybień
24.	04-05.03.2015 DIS-K-421/25/15	Verdict Sp. z o.o. Konstancin – Jeziorna, ul. Spokojna 6	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
25.	04-06.03.2015 DIS-K-421/26/15	Integracyjne Centrum Dydaktyczno – Sportowe w Łomiankach, Łomianki, ul. Staszica 2	z urzędu	przywrócono stan zgodny z prawem
26.	04-06.03.2015 DIS-K-421/27/15	Miejski Ośrodek Sportu i Rekreacji w Sochaczewie, Sochaczew, ul. Olimpijska 3	z urzędu	nie stwierdzono uchybień
27.	04-06.03.2015 DIS-K-421/28/15	Miejski Ośrodek Sportu i Rekreacji w Mińsku Maz. Mińsk Mazowiecki ul. Wyszyńskiego 56	z urzędu	nie stwierdzono uchybień
28.	04-05.03.2015 DIS-K-421/29/15	Janusz Kiebasiński prowadzący działalność gospodarczą pod nazwą „Wypożyczalnia Sprzętu Sportowego”, Warszawa, ul. Inspektowa 1	z urzędu	decyzja GIODO
29.	02-05.03.2015 DIS-K-421/30/15	Miejski Ośrodek Sportu i Rekreacji w Łodzi, Łódź, ul. ks. Skorupki 21	z urzędu	nie stwierdzono uchybień
30.	09-13.03.2015 DIS-K-421/31/15	CebitGroup EP Sp. z o.o. sp. j. Wrocław, ul. Kominiarska 42B	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
31.	11-13.03.2015 DIS-K-421/32/15	Info Veriti Polska Sp. z o.o. Obsługa Serwisu Internetowego sp. j. Warszawa, ul. Serwituty 23	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
32.	12-13.03.2015 DIS-K-421/33/15	Tomasz Jędrzejewski i Witold Jędrzejewski Piruet s.c. Warszawa, ul. Żabińskiego 9/26	z urzędu	nie stwierdzono uchyb4ień

33.	16-20.03.2015 DIS-K-421/34/15	Samodzielny Publiczny Zakład Opieki Zdrowotnej „Szpital Powiatowy w Kętrzynie”, Kętrzyn, ul. Skłodowskiej – Curie 2	Prokuratura Rejonowa w Kętrzynie	decyzja GIODO
34.	16-20.03.2015 DIS-K-421/35/15	Zakopiańskie Towarzystwo Gospodarcze Sp. z o.o. Zakopane, ul. Zwierzyniecka 14	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
35.	16-20.03.2015 DIS-K-421/36/15	Ministerstwo Sprawiedliwości, Warszawa, Al. Ujazdowskie 11	z urzędu	w toku
36.	16.03.2015 DIS-K-421/37/15	Sławomir Hess prowadzący działalność gospodarczą pod nazwą „Modelina Sławomir Hess”, Goczałkowice – Zdrój, ul. Szkolna 79	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
37.	23-30.03.2015 DIS-K-421/38/15	GoWork.pl Serwis Pracy Sp. z o.o. Warszawa, ul. Żurawia 47	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
38.	23-30.03.2015 DIS-K-421/39/15	Andrzej Kosieradzki prowadzący działalność gospodarczą pod nazwą „GoWork.pl Andrzej Kosieradzki”, Warszawa, ul. Żurawia 47	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem
39.	23-27.03.2015 DIS-K-421/40/15	Mariusz Borkowski prowadzący działalność gospodarczą pod nazwą „Przedsiębiorstwo Produkcyjno – Handlowo – Usługowe BOR-POL Mariusz Borkowski”, Gliwice, ul. Jaśminu 2	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
40.	23-27.03.2015 DIS-K-421/41/15	Barbara Stuglik prowadząca działalność gospodarczą pod nazwą „COBA Barbara Stuglik”, Sośnicowice, ul. Raciborska 9	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
41.	23-26.03.2015 DIS-K-421/42/15	Mazowiecka Jednostka Wdrażania Programów Unijnych, Warszawa, ul. Jagiellońska 74	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
42.	25.03.2015 DIS-K-421/43/15	Cifial Polska Sp. z o.o. Warszawa, ul. Białołęcka 168	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
43.	24-27.03.2015 DIS-K-421/44/15	Prezes Urzędu Ochrony Konkurencji i Konsumentów, Warszawa, Pl. Powstańców Warszawy 1	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
44.	08-10.04.2015 DIS-K-421/45/15	Beata Czachorowska prowadząca działalność gospodarczą pod nazwą „Ośrodek Rehabilitacyjno – Sportowy FIT & FUN Beata Czachorowska”, Warszawa, ul. Wysockiego 51	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
45.	08-10.04.2015 DIS-K-421/46/15	Muzeum Powstania Warszawskiego, Warszawa, ul. Grzybowska 79	Departament Orzecznictwa Legislacji i Skarg	przywrócono stan zgodny z prawem

46.	09-10.04.2015 DIS-K-421/47/15	Cyfrowy Polsat S.A. Warszawa, ul. Łubinowa 4A	z urzędu	decyzja GIODO
47.	09-10.04.2015 DIS-K-421/48/15	Polkomtel Sp. z o.o. Warszawa, ul. Postępu 3	z urzędu	decyzja GIODO
48.	13-17.04.2015 DIS-K-421/49/15	Prezydent m.st. Warszawy, Warszawa, ul. Sandomierska 12	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
49.	13-17.04.2015 DIS-K-421/50/15	Alektum Inkasso Sp. z o.o. Wrocław, ul. Kilińskiego 30	Departament Edukacji Społecznej i Współpracy Międzynarodowej	wnioski przekazano do Departamentu Edukacji Społecznej i Współpracy Międzynarodowej
50.	15-17.04.2015 DIS-K-421/51/15	Orange Polska S.A. Warszawa, Al. Jerozolimskie 160	z urzędu	decyzja GIODO
51.	20-24.04.2015 DIS-K-421/52/15	Business Lease Poland Sp. z o.o. Warszawa, ul. Taśmowa 7	z urzędu	decyzja GIODO
52.	20-24.04.2015 DIS-K-421/53/15	Miejski Ośrodek Pomocy Społecznej w Łodzi, Łódź, ul. Piotrkowska 149	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
53.	20-24.04.2015 DIS-K-421/54/15	Ministerstwo Finansów, Warszawa, ul. Świętokrzyska 12	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
54.	20-22.04.2015 DIS-K-421/55/15	Google Poland Sp. z o.o. Warszawa, ul. Emilii Plater 53	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
55.	20-24.04.2015 DIS-K-421/56/15	Natur Produkt Zdrovit Sp. z o.o. Warszawa, ul. Nocznickiego 31	z urzędu	nie stwierdzono uchybień
56.	27-30.04.2015 DIS-K-421/57/15	Dom Pomocy Społecznej, Ciechanów, ul. Krucza 32	Mazowiecki Urząd Wojewódzki	nie stwierdzono uchybień
57.	27-30.04.2015 DIS-K-421/58/15	H+H Polska Sp. z o.o. Warszawa, ul. Kupiecka 6	z urzędu	nie stwierdzono uchybień
58.	27-30.04.2015 DIS-K-421/59/15	Janina Kamieńska, Jacek Jurczewski, Marcin Osuchowski, Zbigniew Skibiński Zakład Elektroniki „ISKO”, Żyrardów, ul. Zielińskiej 36A	z urzędu	w toku
59.	28-30.04.2015 DIS-K-421/61/15	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	z urzędu	decyzja GIODO
60.	28.04.2015 DIS-K-421/62/15	Althermedia Sp. z o.o. sp. k. Warszawa, Al. Niepodległości 201 lok. 25	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
61.	04-08.05.2015 DIS-K-421/63/15	Avrio Sp. z o.o. Rzeszów, ul. Langiewicza 29	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
62.	04-08.05.2015 DIS-K-421/64/15	MPM Maria Kokoczka i Mirosław Prucnal sp. j. Jasło, ul. Jana Pawła II 26	Departament Rejestracji Zbiorów Danych Osobowych	decyzja GIODO
63.	06-08.05.2015 DIS-K-421/65/15	Poczta Polska S.A., Warszawa, ul. Stawki 2	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
64.	11-22.05.2015 DIS-K-421/66/15	Urząd ds. Cudzoziemców, Warszawa, ul. Koszykowa 16	z urzędu	w toku
65.	11-22.05.2015 DIS-K-421/67/15	Urząd ds. Cudzoziemców, Warszawa, ul. Koszykowa 16	z urzędu	w toku
66.	11-15.05.2015 DIS-K-421/68/15	Stowarzyszenie na Rzecz Osób Wykluczonych i Zagrożonych	Departament Rejestracji Zbiorów	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych

		Wykluczeniem Społecznym „Podwale Siedem”, Wrocław, ul. Wszystkich Świętych 2	Danych Osobowych	
67.	11-13.05.2015 DIS-K-421/69/15	Kodak Polska Sp. z o.o. Warszawa, ul. Domaniewska 50	z urzędu	decyzja GIODO
68.	25-29.05.2015 DIS-K-421/70/15	Mediporta Sp. z o.o. Poznań, ul. Marcelińska 90	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
69.	12-15.05.2015 DIS-K-421/71/15	Eurobus Sp. z o.o. Katowice, ul. Pukowca 15	w związku z kontrolą DIS-K-421/148/14	nie stwierdzono uchybień
70.	18-22.05.2015 DIS-K-21/72/15	Paymento S.A. Tychy, ul. Dojazdowa 9	Departament Rejestracji Zbiorów Danych Osobowych	w toku
71.	18-19.05.2015 DIS-K-421/73/15	Queenie Sp. z o.o. Warszawa, Al. Solidarności 117 lok. 207	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
72.	25-29.05.2015 DIS-K-421/74/15	BSP S.A. Łódź, ul. Pabianicka 94/96	z urzędu	nie stwierdzono uchybień
73.	25-27.05.2015 DIS-K-421/75/15	Fideus Sp. z o.o. Warszawa, ul. Czerniakowska 71	z urzędu	nie stwierdzono uchybień
74.	25-29.05.2015 DIS-K-421/76/15	Wydział Konsularny Ambasady RP w Republice Turcji, Ankara, Atatürk Bulvari 241	z urzędu	przywrócono stan zgodny z prawem
75.	25-28.05.2015 DIS-K-421/77/15	Przedsiębiorstwo Usługowo – Handlowe Budowy i Naprawy Dróg „Efekt” Sp. z o.o. Warszawa, ul. Szomańskiego 8	z urzędu	nie stwierdzono uchybień
76.	25-29.05.2015 DIS-K-421/78/15	Polskie Młyny S.A. Koprki, ul. Jaśminowa 27	z urzędu	decyzja GIODO
77.	29.05-03.06.2015 DIS-K-421/79/15	Archiwista Sp. z o.o. Teresin, ul. 1 Maja 45	z urzędu	decyzja GIODO
78.	08-12.06.2015 DIS-K-421/80/15	Centrum Turystyczno – Sportowe Sp. z o.o. Nowa Ruda, ul. Kłodzka 16	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
79.	08-12.06.2015 DIS-K-421/81/15	Burmistrz Miasta Nowa Ruda, Nowa Ruda, ul. Rynek 1	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
80.	09-10.06.2015 DIS-K-421/82/15	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
81.	15-19.06.2015 DIS-K-421/83/15	Wydział Konsularny Ambasady RP w Londynie, Londyn, 47 Portland Place	z urzędu	przywrócono stan zgodny z prawem
82.	15-19.06.2015 DIS-K-421/84/15	Biuro Poselskie Posła Mieczysława Golby, Jarosław, Rynek 6	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
83.	22-25.06.2015 DIS-K-421/85/15	Concorde Investissement S.A. Warszawa, ul. Emilii Plater 18	z urzędu	nie stwierdzono uchybień
84.	22-23.06.2015 DIS-K-421/86/15	Zenon Giżycki, Nadarzyn, Pl. Poniatowskiego 9 m. 4	z urzędu	nie stwierdzono uchybień
85.	22-26.06.2015 DIS-K-421/87/15	State Street Bank GmbH Sp. z o.o. Oddział w Polsce, Kraków, ul. Podgórska 36	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
86.	29.06-03.07.2015 DIS-K-421/88/15	TOM-MARG ZPCH Sp. z o.o. Kraków, ul. Dąbka 16	z urzędu	nie stwierdzono uchybień

87.	29.06-03.07.2015 DIS-K-421/89/15	Waldemar Michalec prowadzący działalność gospodarczą pod nazwą „Dokumenta Waldemar Michalec”, Radom, ul. Kasztelańska 36a lok. 1	z urzędu	przywrócono stan zgodny z prawem
88.	29.06-03.07.2015 DIS-K-421/90/15	Instytut Szkoleń i Analiz S.A. Warszawa, Al. Jana Pawła II 27	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
89.	29.06-03.07.2015 DIS-K-421/91/15	Plus Bank S.A. Warszawa, Al. Stanów Zjednoczonych 61A	z urzędu	nie stwierdzono uchybień
90.	29.06-03.07.2015 DIS-K-421/92/15	Schober Information Group Polska Sp. z o.o. Warszawa, ul. Lesznowolska 6A	w związku z kontrolą DIS-K-421/20/15	nie stwierdzono uchybień
91.	30.06-06.07.2015 DIS-K-421/93/15	Alior Bank S.A. Warszawa, ul. Łopuszańska 38d	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
92.	06-10.07.2015 DIS-K-421/94/15	Urząd Gminy Wieliszew, Wieliszew, ul. Modlińska 1	z urzędu	decyzja GIODO
93.	06-09.07.2015 DIS-K-421/95/15	Foxberg Sp. z o.o. Częstochowa, ul. Dekabrystów 82	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
94.	08-09.07.2015 DIS-K-421/96/15	SRS s.c. Stanisław Drozd, Rafał Zakrzewski, Kraków, ul. Wrocławska 37A lok. 506	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
95.	13-17.07.2015 DIS-K-421/97/15	Zakład Doświadczalny Rossocha Sp. z o.o. Rossocha 1	z urzędu	nie stwierdzono uchybień
96.	13-17.07.2015 DIS-K-421/98/15	Regionalne Centrum Krwiodawstwa i Krwiolecznictwa im. dr Konrada Vietha w Radomiu SP ZOZ, Radom, ul. Limanowskiego 42	z urzędu	decyzja GIODO
97.	20-24.07.2015 DIS-K-421/99/15	Regionalne Centrum Krwiodawstwa i Krwiolecznictwa w Gdańsku SP ZOZ, Gdańsk, ul. Wrońskiego 4	z urzędu	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
98.	20-24.07.2015 DIS-K-421/100/15	MNI Centrum Usług S.A. Radom, ul. Potkanowska 54A	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
99.	20-24.07.2015 DIS-K-421/101/15	Wójt Gminy Jabłonna, Jabłonna, ul. Modlińska 152	z urzędu	nie stwierdzono uchybień
100.	27-31.07.2015 DIS-K-421/102/15	Prezydent Miasta Łodzi, Łódź, ul. Piotrkowska 104	z urzędu	nie stwierdzono uchybień
101.	27-31.07.2015 DIS-K-421/103/15	Centralne Laboratorium Kryminalistyczne Policji, Warszawa, Al. Ujazdowskie 7	z urzędu	w toku
102.	27-31.07.2015 DIS-K-421/104/15	Urząd Miejski w Łomiankach, Łomianki, ul. Warszawska 115	z urzędu	nie stwierdzono uchybień
103.	27-31.07.2015 DIS-K-421/105/15	ABB Sp. z o.o. Warszawa, ul. Żegańska 1	z urzędu	decyzja GIODO
104.	10-13.08.2015 DIS-K-421/107/15	Ministerstwo Pracy i Polityki Społecznej, Warszawa, ul. Nowogrodzka 1/3/5	z urzędu	nie stwierdzono uchybień
105.	17-21.08.2015 DIS-K-421/109/15	Meble – Black Red White Sp. z o.o. Biłgoraj,	z urzędu	w toku

		ul. Krzeszowska 61		
106.	17-21.08.2015 DIS-K-421/110/15	Black Red White S.A. Biłgoraj, ul. Krzeszowska 61	z urzędu	w toku
107.	17-21.08.2015 DIS-K-421/111/15	Urząd Gminy w Stegnie, Stegny, ul. Gdańska 34	z urzędu	nie stwierdzono uchybień
108.	17-21.08.2015 DIS-K-421/112/15	Burmistrz Miasta Milanówka, Milanówek, ul. Kościuszki 45	z urzędu	decyzja GIODO
109.	17-21.08.2015 DIS-K-421/113/15	Urząd Miasta Marki, Marki, Al. Piłsudskiego 95	z urzędu	nie stwierdzono uchybień
110.	24-28.08.2015 DIS-K-421/114/15	Mobime Sp. z o.o. Warszawa, ul. Wróbla 24 lok. 2	w związku z kontrolą DIS-K-421/20/15	decyzja GIODO
111.	24-28.08.2015 DIS-K-421/115/15	Polska Wytwórnia Papierów Wartościowych S.A. Warszawa, ul. Sanguszki 1	z urzędu	nie stwierdzono uchybień
112.	24-28.08.2015 DIS-K-421/116/15	Burmistrz Makowa Podhalańskiego, Maków Podhalański, ul. Szpitalna 3	z urzędu	decyzja GIODO
113.	24-27.08.2015 DIS-K-421/117/15	MailGrupowy.pl, Kraków, Rynek Główny 28	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
114.	24-31.08.2015 DIS-K-421/118/15	Placówka Straży Granicznej Warszawa - Okęcie, Warszawa, ul. 17 stycznia 45D	z urzędu	w toku
115.	31.08-04.09.2015 DIS-K-421/119/15	Ministerstwo Spraw Zagranicznych, Warszawa, Al. Szucha 23	z urzędu	przywrócono stan zgodny z prawem
116.	31.08-04.09.2015 DIS-K-421/120/15	Wójt Gminy Nieporęt, Nieporęt, Pl. Wolności 1	z urzędu	nie stwierdzono uchybień
117.	07-08.09.2015 DIS-K-421/121/15	GoWork.pl Serwis Pracy Sp. z o.o. Warszawa, ul. Żurawia 47	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
118.	07-11.09.2015 DIS-K-421/122/15	mBank S.A. Warszawa, ul. Senatorska 18	Departament Orzecznictwa Legislacji i Skarg	w toku
119.	14-18.09.2015 DIS-K-421/123/15	P4 Sp. z o.o. Warszawa, ul. Taśmowa 7	Departament Orzecznictwa Legislacji i Skarg	w toku
120.	14-18.09.2015 DIS-K-421/124/15	Vivus Finance Sp. z o.o. Warszawa, ul. 17 Stycznia 56	Departament Rejestracji Zbiorów Danych Osobowych	w toku
121.	14-16.09.2015 DIS-K-421/125/15	Andrzej Czachor prowadzący działalność gospodarczą pod nazwą „Czachor Andrzej Best Partner”, Opole, ul. Dunikowskiego 16c	Departament Orzecznictwa Legislacji i Skarg	zawiadomienie o przestępstwie
122.	14-16.09.2015 DIS-K-421/126/15	Ewa Korcz prowadząca działalność gospodarczą pod nazwą „Ewa Beata Korcz Betakor Zarządzanie Nieruchomościami”, Warszawa, ul. Ciszewska 19 lok. 1	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
123.	22-25.09.2015 DIS-K-421/127/15	P&H Limited Sp. z o.o. Gdańsk, ul. Meissnera 1	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
124.	28.09-02.10.2015 DIS-K-421/128/15	Burmistrz Miasta Nowy Dwór Mazowiecki, Nowy Dwór Mazowiecki,	z urzędu	nie stwierdzono uchybień

		ul. Zakroczymska 30		
125.	28.09-02.10.2015 DIS-K-421/129/15	Placówka Straży Granicznej w Terespolu, Terespol, ul. Wojska Polskiego 164	z urzędu	w toku
126.	28.09-02.10.2015 DIS-K-421/130/15	II Liceum Ogólnokształcące im. Zamoyskiego, Lublin, ul. Ogrodowa 16	z urzędu	przywrócono stan zgodny z prawem
127.	30.09.2015 DIS-K-421/133/15/SPR 1	Rzecznik Praw Obywatelskich, Warszawa, Al. Solidarności 77	sprawdzenie	w toku
128.	05-07.10.2015 DIS-K-421/134/15	First Data Polska S.A. Warszawa, Al. Jerozolimskie 92	w związku z kontrolą DIS-K-421/72/15	ustalenia wykorzystano w postępowaniu DIS-K-421/72/15
129.	06-08.10.2015 DIS-K-421/135/15	Facebook Poland Sp. z o.o. Warszawa, ul. Bielańska 12	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
130.	06-09.10.2015 DIS-K-421/136/15	Samodzielny Zespół Publicznych Zakładów Lecznictwa Otwartego Warszawa - Ochota, Warszawa, ul. Szczęśliwicka 36	z urzędu	nie stwierdzono uchybień
131.	12-16.10.2015 DIS-K-421/137/15	Super-Pharm Poland Sp. z o.o. Warszawa, ul. Domaniewska 39	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
132.	12-16.10.2015 DIS-K-421/139/15	Komenda Powiatowa Policji w Mińsku Mazowieckim, Mińsk Mazowiecki, ul. Wyszyńskiego 15/17	z urzędu	w toku
133.	19-24.10.2015 DIS-K-421/140/15	Referat Konsularny Ambasady RP w Gruzji, Tbilisi, Br. Zubalashvili	z urzędu	przywrócono stan zgodny z prawem
134.	19-22.10.2015 DIS-K-421/141/15	Pharmacy Sp. z o.o. Warszawa, ul. Widna 1E	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
135.	19-23.10.2015 DIS-K-421/142/15	Drzewiecki, Tomaszek i Wspólnicy sp. k. Warszawa, ul. Belwederska 23	z urzędu	nie stwierdzono uchybień
136.	27-30.10.2015 DIS-K-421/143/15	Edukacyjna Fundacja im. prof. Romana Czerneckiego EFC, Warszawa, ul. Mokotowska 63 lok. 60	Departament Rejestracji Zbiorów Danych Osobowych	w toku
137.	26-30.10.2015 DIS-K-421/144/15	Polguard Consulting Sp. z o.o. Turek, ul. Jedwabnicza 4	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Rejestracji Zbiorów Danych Osobowych
138.	26-30.10.2015 DIS-K-421/145/15	NZOZ Zdrowie – Legionowo, Legionowo, ul. Sowińskiego 15A	z urzędu	decyzja GIODO
139.	26-29.10.2015 DIS-K-421/146/15	Artur Glass – Brudziński prowadzący działalność gospodarczą pod nazwą „Glass – Brudziński Artur Adwokaci i Radcy Prawni”, Warszawa, ul. Łucka 15 lok. 1001	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
140.	02-06.11.2015 DIS-K-421/147/15	Burmistrz Miasta Mińsk Mazowiecki, Mińsk Mazowiecki, ul. Konstytucji 3 Maja 1	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
141.	02-06.11.2015 DIS-K-421/148/15	Centrum Medyczne im. Bitwy Warszawskiej 1920 r. w Radzyminie SP ZOZ, Radzymin,	z urzędu	nie stwierdzono uchybień

		ul. Konstytucji 3 Maja 17		
142.	02-06.11.2015 DIS-K-421/149/15	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Sulejówku, Sulejówek, ul. Idzikowskiego 7b	z urzędu	nie stwierdzono uchybień
143.	02-06.11.2015 DIS-K-421/150/15	SP Specjalistyczny Szpital w Grodzisku Mazowieckim, Grodzisk Mazowiecki, ul. Daleka 11	z urzędu	nie stwierdzono uchybień
144.	02-06.11.2015 DIS-K-421/151/15	Ministerstwo Sprawiedliwości, Warszawa, Al. Ujazdowskie 11	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
145.	09-13.11.2015 DIS-K-421/152/15	Ministerstwo Sportu i Turystyki, Warszawa, ul. Senatorska 14	Departament Rejestracji Zbiorów Danych Osobowych	w toku
146.	09-13.11.2015 DIS-K-421/153/15	BPO Poland Sp. z o.o. Warszawa, ul. Długa 29 lok. 226	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
147.	16-20.11.2015 DIS-K-421/154/15	Szef Służby Celnej, Warszawa, ul. Świętokrzyska 12	Departament Edukacji Społecznej i Współpracy Międzynarodowej	w toku
148.	16-20.11.2015 DIS-K-421/155/15	Sąd Apelacyjny we Wrocławiu, Wrocław, ul. Energetyczna 4	Departament Orzecznictwa Legislacji i Skarg	w toku
149.	16-20.11.2015 DIS-K-421/156/15	Dino Polska S.A. Wielka Wieś, ul. Liliowa 2	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
150.	23-27.11.2015 DIS-K-421/157/15	Oskar Wyszyński prowadzący działalność gospodarczą pod nazwą „Oskar Wyszyński Niepubliczny Zakład Opieki Zdrowotnej REH-MED”, Ossy, ul. Leśna 20	Prokuratura Rejonowa w Chorzowie	nie stwierdzono uchybień
151.	23-27.11.2015 DIS-K-421/158/15	Samodzielny Zespół Publicznych Zakładów Lecznictwa Otwartego Warszawa – Targówek, Warszawa, ul. Tykocińska 34	z urzędu	nie stwierdzono uchybień
152.	23-27.11.2015 DIS-K-421/159/15	Termy Maltańskie Sp. z o.o. Poznań, ul. Termalna 1	Rzecznik Praw Obywatelskich	nie stwierdzono uchybień
153.	19.11.2015 DIS-K-421/161/15/SPR 2	Volkswagen Bank Polska S.A. Warszawa, Rondo ONZ 1	sprawdzenie	w toku
154.	24-25.11.2015 DIS-K-421/162/15	Komenda Rejonowa Policji Warszawa VII, Warszawa, ul. Grenadierów 73/75	z urzędu	w toku
155.	26-27.11.2015 DIS-K-421/163/15	Komenda Rejonowa Policji w Garwolinie, Garwolin, ul. Stacyjna 23	z urzędu	w toku
156.	20.11.2015 DIS-K-421/164/15/SPR 3	DNB Bank Polska S.A. Warszawa, ul. Postępu 15C	sprawdzenie	w toku
157.	20.11.2015 DIS-K-421/165/15/SPR 4	Narodowy Bank Polski, Warszawa, Pl. Powstańców Warszawy 4	sprawdzenie	w toku
158.	20.11.2015 DIS-K-421/166/15/SPR 5	ABS Bank Spółdzielczy, Andrychów, ul. Krakowska 112	sprawdzenie	w toku

159.	20.11.2015 DIS-K-421/167/15/SPR 6	Bank Spółdzielczy w Białogardzie, Białogard, ul. Kochanowskiego 6	sprawdzenie	w toku
160.	20.11.2015 DIS-K-421/168/15/SPR 7	mBank S.A. Warszawa, ul. Senatorska 18	sprawdzenie	w toku
161.	03-04.12.2015 DIS-K-421/169/15	Komenda Rejonowa Policji w Wołominie, Wołomin, ul. Wileńska 43A	z urzędu	w toku
162.	03-04.12.2015 DIS-K-421/170/15	Komenda Miejska Policji w Siedlcach, Siedlce, ul. Starowiejska 66	z urzędu	w toku
163.	07-11.12.2015 DIS-K-421/171/15	Wojskowa Specjalistyczna Przychodnia Lekarska SP ZOZ w Legionowie, Legionowo, ul. Zegrzyńska 8	z urzędu	decyzja GIODO
164.	07-11.12.2015 DIS-K-421/172/15	Wydział Konsularny Ambasady RP w Madrycie, Madryt, Guisando 23 bis	z urzędu	przywrócono stan zgodny z prawem
165.	07-11.12.2015 DIS-K-421/173/15	Giełda Papierów Wartościowych w Warszawie S.A. Warszawa, ul. Książęca 4	Prokuratura Rejonowa Warszawa – Śródmieście	wnioski przekazano do Prokuratury Rejonowej Warszawa – Śródmieście
166.	14-18.12.2015 DIS-K-421/203/15	TradeDoubler Sp. z o.o. Warszawa, ul. Piękna 28/34	Departament Rejestracji Zbiorów Danych Osobowych	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
167.	14-18.12.2015 DIS-K-421/204/15	Komenda Główna Straży Granicznej, Warszawa, Al. Niepodległości 100	z urzędu	w toku
168.	17-18.12.2015 DIS-K-421/206/15	Komenda Rejonowa Policji Warszawa VI, Warszawa, ul. Jagiellońska 51	z urzędu	w toku
169.	17-18.12.2015 DIS-K-421/207/15	Komenda Powiatowa Policji w Legionowie, Legionowo, ul. Jagiellońska 26B	z urzędu	w toku
170.	15.12.2015 DIS-K-421/208/15/SPR 8	Bieszczadzki Bank Spółdzielczy w Ustrzykach Dolnych, Ustrzyki Dolne, ul. Bełska 12	sprawdzenie	w toku
171.	15.12.2015 DIS-K-421/209/15/SPR 9	Bank Spółdzielczy Pojezierza Międzychodzko – Sierakowskiego w Sierakowie, Sieraków, ul. Chrobrego 6	sprawdzenie	w toku
172.	15.12.2015 DIS-K-421/210/15/SPR 10	Bank Spółdzielczy w Siedlcu, Siedlec, ul. Zbąszyńska 25	sprawdzenie	w toku
173.	15.12.2015 DIS-K-421/211/15/SPR 11	Bank Spółdzielczy w Nowym Tomyślu, Nowy Tomyśl, ul. Piłsudskiego 2	sprawdzenie	w toku
174.	16.12.2015 DIS-K-421/212/15/SPR 12	Bank Spółdzielczy w Przemkowie, Przemkowo, ul. Głogowska 12A	sprawdzenie	w toku
175.	16.12.2015 DIS-K-421/213/15/SPR 13	Bank Spółdzielczy w Kamiennej Górze, Kamienna Góra, ul. Waryńskiego 11	sprawdzenie	w toku

Załącznik nr 3

Wykaz orzeczeń wydanych w 2015 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.	07.01.2015 r. II SAB/Wa 1130/14	DOLiS-440-394/10	Skarga na bezczynność organu	Postanowienie WSA – odrzucenie skargi
2.	14.01.2015 r. II SA/Wa 791/14	DOLiS/DEC-1367/12/ 17111,17117	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji i określenie, że nie podlega ona wykonaniu w całości
3.	16.01.2015 r. II SA/Wa 1023/14	DOLiS/DEC-388/13/ 24580, 24591, 24601	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na udostępnianie danych osobowych	Wyrok WSA- oddalenie skargi
4.	19.01.2015 r. I OSK 2841/14	DOLiS/DEC-1355/12/4152,4153	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 18.07.2014 r., sygn. akt II SA/Wa 569/14 w sprawie skargi na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie NSA – umorzenie postępowania z art. 161 Ppsa
5.	19.01.2015 r. I OSK 2846/14	DOLiS/DEC-1461/12/4154,4156	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 18.07.2014 r., sygn. akt II SA/Wa 570/14 w sprawie skargi na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie NSA – umorzenie postępowania z art. 161 Ppsa
6.	19.01.2015 r. I OSK 1099/13	DOLiS/DEC-373/12/ 27562, 27570	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 24.01.2013 r. sygn. akt II SA/Wa 1242/12 w sprawie skargi na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 24.01.2013 r. sygn. akt II SA/Wa 1242/12 i oddalający skargę
7.	22.01.2015 r. I OSK 1161/13	DOLiS/DEC-996/12/ 62407,62423,62425,62429,62431	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 25.02.2013 r. sygn. akt II SA/Wa 2267/12 w sprawie decyzji w przedmiocie nakazania udostępnienia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 25.02.2013 r. sygn. akt II SA/Wa 2267/12
8.	29.01.2015 r. II SA/Wa 790/14	DOLiS/DEC-757/12/ 12402,12408,12411	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA- oddalenie skargi
9.	10.02.2015 r. II SAB/Wa 302/15	dot. DOLiS-035-4308/13	Skarga na bezczynność Generalnego Inspektora Ochrony	Postanowienie WSA – odrzucenie skargi

			Danych Osobowych w przedmiocie udzielenia porady prawnej	
10.	10.02.2015 r. II SAB/Wa 547/14	DOLiS-440-1525/12	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA – odrzucenie skargi
11.	11.02.2015 r. I OSK 1164/14	DOLiS-440-102/13	Skarga na bezczynność organu	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 27 .01.2014 r. sygn. akt II SAB/Wa 537/13 w sprawie ze skargi na bezczynność Generalnego Inspektora Ochrony Danych Osobowych
12.	12.02.2015 r. II SAB/Wa 586/14	DOLiS-440-1126/12	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA stwierdzający, iż przewlekłość miała miejsce z rażącym naruszeniem prawa, wymierzający grzywnę w wysokości 3000 zł
13.	12.02.2015 r. II SA/Wa 1502/14	DOLiS/DEC-507/14/ 41187, 41198	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Wyrok WSA- oddalenie skargi
14.	16.02.2015 r. II SA/Wa 1242/14	DOLiS/DEC-675/13/33391, 33397	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji i określenie, że nie podlega ona wykonaniu w całości
15.	19.02.2015 r. II SA/Wa 2008/14	DOLiS/DEC-102/10/ 29711,29715,29717	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie udostępnienia danych osobowych	Wyrok WSA- oddalenie skargi
16.	23.02.2015 r. II SAB/Wa 1132/14	DOLiS-440-1657/14	Skarga na bezczynność organu	Postanowienie WSA – odrzucenie skargi
17.	25.02.2015 r. II SAB/Wa 1069/14	Dot. GI-DS-430/614/02	Skarga o wznowienie postępowania sądowego zakończonego prawomocnym wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 4.12.2013 r., sygn. akt II SAB/Wa 343/13	Postanowienie WSA – odrzucenie skargi
18.	2.03.2015 r. II SA/Wa 998/14	DOLiS/DEC-102/10/ 24587, 24589, 24592, 24595	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA – oddalenie skarg
19.	3.03.2015 r. II SAB/Wa 270/15	DOLiS-440-1552/13	Skarga na bezczynność organu	Postanowienie WSA – odrzucenie skargi
20.	6.03.2015 r. II SA/Wa 1443/14	DOLiS/DEC-869/11/40329, 40334	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
21.	10.03.2015 r. II SA/Wa 1000/14	DOLiS/DEC-483/12/20677,20679,20682	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
22.	10.03.2015 r. II SA/Wa 1310/14	DOLiS/DEC-139/13/44541,44809	Skarga na decyzję w przedmiocie umorzenia postępowania w procesie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
23.	10.03.2015 r. II SAB/Wa 285/15	dot. DOLiS-440-1640/14	Skarga na bezczynność organu	Postanowienie WSA – odrzucenie skargi
24.	11.03.2015 r.	DOLiS/DEC-	Skarga na decyzję w przedmiocie	Wyrok WSA – oddalenie skargi

	II SA/Wa 2188/14	428/10/38752,38755,38759	odmowy uwzględnienia wniosku na udostępnianie danych osobowych	
25.	24.03.2015 r. I OSK 1426/13	DOLiS/DEC-629/10/57034	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 12.03.2013 r. sygn. akt II SA/Wa 2126/12 w sprawie postanowienia w przedmiocie odmowy sporządzenia odpisów wszystkich dokumentów znajdujących się w aktach sprawy	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 12.03.2013 r. sygn. akt II SA/Wa 2126/12
26.	26.03.2015 r. II SA/Wa 1768/14	DOLiS/DEC-1066/13/55583,55584	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie nieprawidłowości w procesie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
27.	31.03.2015 r. I OSK 1805/13	DOLiS/DEC-84/12/56856,56858	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Postanowienie NSA – umorzenie postępowania z art. 161 Ppsa
28.	01.04.2015 r. II SA/Wa 841/14	DOLiS/DEC-394/10/13124,13128,13132,13134	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
29.	02.04.2015 r. I OSK 1814/13	DOLiS/DEC-1156/11/71143,71149,71151,71159	Skarga GIODO od wyroku WSA w Warszawie z dnia 18.04.2013 r. o sygn. akt II SA/Wa 190/13 w sprawie decyzji w przedmiocie odmowy uwzględnienia wniosku w sprawie przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 18.04.2013 r. o sygn. akt II SA/Wa 190/13
30.	02.04.2015 r. I OSK 1760/13	DIS/DEC-847/12/55105	Niezapewnienie możliwości wyboru w zakresie udzielenia bądź nieudzielenia zgody na przetwarzanie danych w celach marketingowych, przetwarzanie danych osób, które nie wyraziły zgody na przetwarzanie danych osobowych lub taką zgodę odwołały, niezapewnienie, aby dane były przechowywane w postaci umożliwiającej identyfikację osób nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania danych.	oddalenie skargi kasacyjnej
31.	9.04.2015 r. I OSK 2926/13	DOLiS/DEC-1087/11/72653,72655	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 13.08.2013 r. sygn. akt II SA/Wa 149/13 w sprawie ze skargi na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie upublicznienia danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 13.08.2013 r. sygn. akt II SA/Wa 149/13 i przekazujący sprawę do ponownego rozpoznania przez WSA
32.	10.04.2015 r. II SA/Wa 458/15	DOLiS/DEC-341/11/23575, 23580, 23585	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA - umorzenie postępowania z art. 161 Ppsa

33.	10.04.2015 r. II SA/Wa 2097/14	DOLiS/POST-785/13/70381	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Wyrok WSA – uchylenie zaskarżonego postanowienia oraz poprzedzającego go postanowienia i określenie, że nie podlegają one wykonaniu w całości
34.	10.04.2015 r. II SAB/Wa 870/14	DOLiS-440-785/13	Skarga na bezczynność organu	Wyrok WSA stwierdzający, iż bezczynność miała miejsce z rażącym naruszeniem prawa i umarzający postępowanie w pozostałym zakresie
35.	13.04.2015 r. II SA/Wa 1527/14	DOLiS/DEC-1185/11/44843, 44857, 44863	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji i określenie, że nie podlega ona wykonaniu w całości
36.	14.04.2015 r. II SAB/Wa 501/14	DOLiS-440-1059/13	Skarga na bezczynność organu	Wyrok WSA stwierdzający, iż bezczynność nie miała miejsca z rażącym naruszeniem prawa i umarzający postępowanie w pozostałym zakresie
37.	21.04.2015 r. II SA/Wa 1865/14	DOLiS/DEC-1618/13/66511,66518	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji i określenie, że nie podlegają one wykonaniu w całości
38.	21.04.2015 r. I OSK 1480/14	DOLiS/DEC-895/12/47061,47062	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 29.01.2014 r. sygn. akt II SA/Wa 1819/13 w sprawie ze skargi na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 29.01.2014 r. sygn. akt II SA/Wa 1819/13
39.	21.04.2015 r. I OSK 2808/14	DOLiS/DEC-983/13/60294,60298	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 2.07.2014 r. sygn. akt II SA/Wa 675/14 w sprawie ze skargi o wymierzenie Generalnemu Inspektorowi Ochrony Danych Osobowych grzywny z tytułu niewykonania wyroku	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 2.07.2014 r. sygn. akt II SA/Wa 675/14
40.	21.04.2015 r. I OSK 1968/13	DOLiS/DEC-189/12/75421,75423	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 16.05.2013 r. sygn. akt II SA/Wa 294/13 w sprawie ze skargi na decyzję w przedmiocie umorzenia postępowania ze skargi na przetwarzanie danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 16.05.2013 r. sygn. akt II SA/Wa 294/13
41.	22.04.2015 r. II SA/Wa 847/14	DOLiS/DEC-207/13/18930,18935	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji i określenie, że nie podlegają one wykonaniu w całości
42.	23.04.2015 r. II SA/Wa 1002/14	DOLiS/DEC-1128/12/24569,24572,24577,24581,24583	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi

43.	23.04.2015 r. II SA/Wa 1844/14	DOLiS/DEC-981/12/58044,58049,58052	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
44.	28.04.2015 r. II SAB/Wa 623/15	DOLiS-440-495/14	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA – odrzucenie skargi
45.	28.04.2015 r. I OZ 375/15	DOLiS/DEC-1125/13/74694,74696	Zażalenie na postanowienie WSA w Warszawie z dnia 29.01.2015 r., sygn. akt II SA/Wa 2095/14 o wstrzymaniu wykonania decyzji w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 29.01.2015 r., sygn. akt II SA/Wa 2095/14 wstrzymaniu wykonania zaskarżonej decyzji
46.	29.04.2015 r. II SA/Wa 1604/14	DOLiS/DEC-462/13/50917,50922	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji i określenie, że nie podlegają one wykonaniu w całości
47.	29.04.2015 r. II SAB/Wa 1133/14	DOLiS-440-157/14	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA – odrzucenie skargi
48.	5.05.2015 r. II SA/Wa 1714/14	DOLiS/DEC-930/12/52969,52975	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji i określenie, że nie podlegają one wykonaniu w całości
49.	5.05.2015 r. II SA/Wa 1998/14	DOLiS/POST-293/14/71753	Skarga na postanowienie w przedmiocie uchybienia terminu do wniesienia zażalenia	Wyrok WSA – uchylenie zaskarżonego postanowienia i określenie, że nie podlega ono wykonaniu w całości
50.	5.05.2015 r. II SAB/Wa 637/14	DOLiS-440-1251/11	Skarga na bezczynność organu	Wyrok WSA – stwierdzający, że bezczynność nie miała miejsca z rażącym naruszeniem prawa i umarzający postępowanie w pozostałym zakresie
51.	6.05.2015 r. I OSK 1538/14	DOLiS-440-981/12	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 10.02.2014 r. sygn. akt II SAB/Wa 566/13 stwierdzającego, że bezczynność miała miejsce z rażącym naruszeniem prawa i wymierzającego grzywnę w wysokości 1000 zł	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 10.02.2014 r. sygn. akt II SAB/Wa 566/13
52.	14.05.2015 r. II SAB/Wa 637/15	…	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA – odrzucenie skargi
53.	19.05.2015 r. II SAB/Wa 1002/14	DOLiS-440-1426/13	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA stwierdzający, iż przewlekłość miała miejsce z rażącym naruszeniem prawa, wymierzający grzywnę w wysokości 2000 zł i umarzający postępowanie w pozostałym zakresie
54.	20.05.2015 r. II SA/Wa 2096/14	DOLiS/DEC-418/12/73275,73286,73300	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Postanowienie WSA – odrzucenie skargi

55.	20.05.2015 r. II SAB/Wa 979/14	DOLiS-440-213/14	Skarga na bezczynność organu	Wyrok WSA – zobowiązujący GIODO do rozpatrzenia skargi na przetwarzanie danych osobowych w terminie 30 dni od daty doręczenia prawomocnego wyroku wraz z aktami sprawy i stwierdzający, że bezczynność miała miejsce z rażącym naruszeniem prawa
56.	20.05.2015 r. I OSK 9/15	DOLiS-440-857/12	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 9.10.2014 r. sygn. akt II SAB/Wa 38/14, w przedmiocie rozpatrzenia skargi w sprawie nieprawidłowości w procesie przetwarzania danych osobowych, stwierdzającego, że bezczynność miała miejsce z rażącym naruszeniem prawa, wymierzającego grzywnę w wysokości 2000 zł i umarzającego postępowanie w pozostałym zakresie	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 9.10.2014 r. sygn. akt II SAB/Wa 38/14
57.	20.05.2015 r. I OZ 479/15	DOLiS/DEC-615/11/57604,57607	Zażalenie na postanowienie WSA w Warszawie z dnia 10.02.2015 r., sygn. akt II SA/Wa 2033/14 o odmowie przywrócenia terminu do wniesienia skargi na decyzję w przedmiocie umorzenia postępowania w sprawie zaniechania obowiązku uaktualnienia danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 10.02.2015 r., sygn. akt II SA/Wa 2033/14
58.	22.05.2015 r. II SAB/Wa 1024/14	DOLiS-440-1827/14	Skarga na bezczynność organu w sprawie, dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
59.	27.05.2015 r. II SA/Wa 1769/14	DOLiS/DEC-1305/12/57405,57407	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
60.	27.05.2015 r. II SA/Wa 1963/14	DOLiS/POST-820/13/66962	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Wyrok WSA – oddalenie skargi
61.	1.06.2015 r. II SAB/Wa 607/15	DOLiS-440-1827/14	Skarga na bezczynność organu w sprawie, dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
62.	3.06.2015 r. II SA/Wa 1950/14	DOLiS/DEC-370/12/73257,73259,73260	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych, zaś w pozostałym zakresie odmawiającą uwzględnienia wniosku w sprawie skargi, na przetwarzanie danych osobowych	Postanowienie WSA – odrzucenie skargi
63.	3.06.2015 r. I OSK 2496/13	DOLiS/DEC-165/12/69181,69183	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 17.06.2013 r. sygn. akt II SA/Wa	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 17.06.2013 r. sygn. akt II

			152/13 oddalającego skargę na decyzję w przedmiocie nakazania udostępnienia danych osobowych, zaś w pozostałym zakresie umarzającą postępowanie	SA/Wa 152/13 i przekazujący sprawę do ponownego rozpoznania przez WSA
64.	9.06.2015 r. II SA/Wa 1999/14	DOLiS/DEC-397/12/73567,73571	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
65.	17.06.2015 r. II SAB/Wa 638/15	DOLiS-440-1683/14	Skarga na przewlekłe prowadzenie postępowania w sprawie, dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
66.	19.06.2015 r. II SA/Wa 2000/14	DOLiS/DEC-804/13/76201,76219	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA – umorzenie postępowania z art. 161 Ppsa
67.	22.06.2015 r. II SA/Wa 1464/14	DOLiS/DEC-1537/12/41182,41183	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
68.	24.06.2015 r. II SA/Wa 1516/14	DOLiS/DEC-….	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
69.	25.06.2015 r. II SAB/Wa 305/15	DOLiS-035-3972/14	Skarga na bezczynność organu	Wyrok WSA – oddalenie skargi
70.	26.06.2015 r. II SA/Wa 800/15	DOLiS/DEC-1681/13/15001,15005	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – odrzucenie skargi
71.	29.06.2015 r. II SAB/Wa 517/15	DOLiS-440-1440/13	Skarga na przewlekłe prowadzenie postępowania w sprawie, dotyczącej przetwarzania danych osobowych w celach marketingowych	Postanowienie WSA – odrzucenie skargi
72.	30.06.2015 r. I OZ 624/15	DOLiS/DEC-90/13/7191,7193	Zażalenie na postanowienie WSA w Warszawie z dnia 15.04.2015 r., sygn. akt II SA/Wa 546/15 o wstrzymaniu wykonania decyzji nakazującej przywrócenie stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 15.04.2015 r., sygn. akt II SA/Wa 546/15
73.	1.07.2015 r. II SA/Wa 2048/14	DOLiS/DEC-410/09/71102,71105,71108, 71109, 71111, 71505, 71521	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
74.	1.07.2015 r. II SA/Wa 2033/14	DOLiS/DEC-615/11/57604,57607	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – odrzucenie skargi
75.	2.07.2015 r. II SAB/Wa 608/15	DOLiS-440-1440/13	Skarga na bezczynność organu	Postanowienie WSA – odrzucenie skargi

76.	2.07.2015 r. II SA/Wa 499/15	DOLiS/POST-1122/14/14834	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Postanowienie WSA – odrzucenie skargi
77.	2.07.2015 r. I OZ 732/15	DOLiS/DEC-323/13/93669,93976	Zażalenie na postanowienie WSA w Warszawie z dnia 20.04.2015 r., sygn. akt II SA/Wa 183/15 o wstrzymaniu wykonania decyzji nakazującej przywrócenie stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 20.04.2015 r., sygn. akt II SA/Wa 183/15
78.	7.07.2015 r. II SA/Wa 449/15	DOLiS/DEC-1252/11/60,62,65,	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
79.	9.07.2015 r. II SA/Wa 2095/14	DOLiS/DEC-1125/13/74694,74696	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji i określenie, że nie podlegają one wykonaniu w całości
80.	10.07.2015 r. I OSK 2498/13	DOLiS/DEC-211/11/3855,3857,3859	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 23.05.2013 r. sygn. akt II SA/Wa 625/13 oddalającego skargę na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 23.05.2013 r. sygn. akt II SA/Wa 625/13
81.	10.07.2015 r. II SA/Wa 2163/14	DIS/DEC-964/14/77489	Udostępnianie danych osobowych innemu podmiotowi bez podstawy prawnej, pozyskiwanie danych osobowych bez podstawy prawnej.	oddalenie skargi
82.	15.07.2015 r. II SA/Wa 2280/14	DIS/DEC-1025/14/84758	Udostępnianie danych osobowych innemu podmiotowi bez podstawy prawnej.	oddalenie skargi
83.	16.07.2015 r. II SA/Wa 1027/15	dot. GI-DS.-430/614/02	Skarga na niewykonanie wyroku WSA w Warszawie z dnia z 4.12.2013 r., sygn. akt II SAB/Wa 343/13	Postanowienie WSA – odrzucenie skargi
84.	17.07.2015 r. I OSK 182/14	DOLiS/DEC-269/12/7457,7461	Skarga kasacyjna GIODO od wyroku WSA z dnia 2.10.2013 r. sygn. akt II SA/Wa 627/13 w sprawie ze skargi na decyzję w przedmiocie nakazania usunięcia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 2.10.2013 r. sygn. akt II SA/Wa 627/13
85.	22.07.2015 r. II SAB/Wa 595/15	DOLiS-440-1657/14	Skarga na bezczynność organu w sprawie, dotyczącej odmowy sprostowania danych osobowych	Postanowienie WSA – odrzucenie skargi
86.	22.07.2015 r. II SA/Wa 658/15	DIS/DEC-71/15/8533	Przetwarzanie danych biometrycznych bez podstawy prawnej.	odmowa wstrzymania wykonania decyzji
87.	18.08.2015 r. II SA/Wa 11/15	DOLiS/DEC-1175/12/83496,83498,83501	Skarga na decyzję w przedmiocie nakazu zaprzestania przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
88.	18.08.2015 r. II SAB/Wa 602/15	DOLiS-440-1657/14	Skarga na bezczynność organu w sprawie, dotyczącej przetwarzania danych	Wyrok WSA – stwierdzający, że bezczynność nie miała miejsca z rażącym naruszeniem prawa i

			osobowych	umarzający postępowanie w pozostałym zakresie
89.	18.08.2015 r. II SO/Wa 153/15	DOLiS-440-1788/14	Wniosek o wymierzenie GIODO grzywny za nieprzekazanie w ustawowym terminie skargi, odpowiedzi na skargę i akt administracyjnych	Postanowienie WSA - odrzucenie wniosku
90.	19.08.2015 r. I OZ 851/15	DOLiS-440-1827/14	Zażalenie na postanowienie WSA w Warszawie z dnia 18.05.2015 r. sygn. akt II SAB/Wa 588/15 o odmowie przyznania prawa pomocy w sprawie ze skargi na bezczynność organu.	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 18.05.2015 r. sygn. akt II SAB/Wa 588/15
91.	26.08.2015 r. II SA/Wa 1089/15	DOLiS/DEC-1682/13/34512,34519	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
92.	26.08.2015 r. I OZ 1007/15	DOLiS/DEC-757/12/12402,12408,12411	Zażalenie na postanowienie WSA w Warszawie z dnia 17.06.2015 r., sygn. akt II SA/Wa 790/14 odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych oraz ustanowienia adwokata w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 17.06.2015 r., sygn. akt II SA/Wa 790/14
93.	27.08.2015 r. II SA/Wa 900/15	DOLiS/DEC-1087/11/72653,72655	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie upublicznienia danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji i określenie, że nie podlega ona wykonaniu w całości
94.	2.09.2015 r. II SA/Wa 1881/14	DOLiS/DEC-21/12/70383,70386	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji
95.	8.09.2015 r. II SA/Wa 34/15	DOLiS/DEC-646/13/83550,83579,83589	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
96.	8.09.2015 r. II SA/Wa 155/15	DOLiS/DEC-1316/12/93703,93705,93706	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na udostępnienie danych osobowych	Wyrok WSA – oddalenie skargi
97.	8.09.2015 r. II SAB/Wa 644/14	DOLiS-440-646/13	Skarga na bezczynność organu w sprawie, dotyczącej wniosku o ponowne rozpatrzenie sprawy dotyczącej skargi na przetwarzania danych osobowych	Wyrok WSA – stwierdzający, że bezczynność nie miała miejsca z rażącym naruszeniem prawa, umarzający postępowanie w pozostałym zakresie i oddalający wniosek o wymierzenie grzywny
98.	8.09.2015 r. II SA/Wa 1302/15	DOLiS/DEC-760/14/49554,49556	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
99.	11.09.2015 r. II SA/Wa 85/15	DOLiS/DEC-1492/12/87527,87518	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na	Wyrok WSA – oddalenie skargi

			udostępnienie danych osobowych	
100.	11.09.2015 r. I OZ 1254/15	DOLiS-440-1827/14	Zażalenie na postanowienie WSA w Warszawie z dnia 1.06.2015 r., sygn. akt II SAB/Wa 607/15 odmawiające przyznania prawa pomocy w sprawie ze skargi na bezczynność organu w sprawie dotyczącej przetwarzania danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 1.06.2015 r., sygn. akt II SAB/Wa 607/15
101.	15.09.2015 r. II SA/Wa 894/15	DOLiS/DEC-793/13/26346,26353	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
102.	16.09.2015 r. II SA/Wa 2139/14	DOLiS/DEC-1512/12/75368,75375	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na nieprawidłowości w procesie przetwarzania danych osobowych	Postanowienie WSA - umorzenie postępowania z art. 161 Ppsa
103.	17.09.2015 r. II SA/Wa 1218/15	DOLiS/DEC-794/14/42035,42045	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
104.	17.09.2015 r. II SAB/Wa 909/15	dot. DOLiS-035-1208/15	Skarga na bezczynność organu w sprawie, dotyczącej rozpoznania wniosku w przedmiocie interpretacji przepisów ustawy o ochronie danych osobowych	Postanowienie WSA – odrzucenie skargi
105.	17.09.2015 r. II SAB/Wa 852/15	DOLiS-440-535/14	Skarga na bezczynność organu w sprawie, dotyczącej przetwarzania danych osobowych przez udostępnienie ich na stronie internetowej	Postanowienie WSA – odrzucenie skargi
106.	23.09.2015 r. II SA/Wa 1533/15	DOLiS/POST-684/14/69887,69890	Skarga na postanowienie w przedmiocie omowy wstrzymania decyzji	Postanowienie WSA – odrzucenie skargi
107.	24.09.2015 r. VIII SA/Wa 124/15	DOLiS/POST-12184/14/97239	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Wyrok WSA – uchylenie zaskarżonego postanowienia oraz poprzedzającego go postanowienia
108.	28.09.2015 r. IV SAB/Wa 405/15	DOLiS-440-1540/15	Skarga na bezczynność organu	Postanowienie WSA – odrzucenie skargi
109.	30.09.2015 r. II SA/Wa 1409/15	DOLiS/DEC-552/15/57825,57835	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji z lipca 2015
110.	30.09.2015 r. I OZ 1071/15	DOLiS-440-1826/14	Zażalenie na postanowienie WSA w Warszawie z dnia 18.06.2015 r., sygn. akt II SAB/Wa 1023/14 odmawiające przyznania prawa pomocy w zakresie zwolnienia od kosztów sądowych w sprawie ze skargi na bezczynność organu w sprawie dotyczącej przetwarzania danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 18.06.2015 r., sygn. akt II SAB/Wa 1023/14
111.	1.10.2015 r. II SA/Wa 1451/15	DOLiS/DEC-627/14/60528,60533	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
112.	5.10.2015 r.	DOLiS/DEC-	Skarga na decyzję w przedmiocie	Wyrok WSA – oddalenie skargi

	II SA/Wa 48/15	16/14/83599,83603,83608	odmowy stwierdzenia nieważności decyzji	
113.	6.10.2015 r. I OZ 1134/15	DOLiS/DEC-1075/14/15589,15591	Zażalenie na postanowienie WSA w Warszawie z dnia 26.05.2015 r., sygn. akt II SA/Wa 659/15 o odmowie wstrzymania wykonania decyzji w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA o uchyleniu postanowienia WSA w Warszawie z dnia 26.05.2015 r., sygn. akt II SA/Wa 659/15 i wstrzymaniu wykonania zaskarżonej decyzji
114.	7.10.2015 r. II SAB/Wa 588/15	DOLiS-440-1827/14	Skarga na bezczynność organu w sprawie, dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi
115.	9.10.2015 r. II SA/Wa 40/15	DOLiS/DEC-845/14/87520,87532	Skarga na decyzję w przedmiocie zaprzestania przetwarzania danych osobowych w celach marketingowych	Wyrok WSA – oddalenie skargi
116.	15.10.2015 r. I OZ 1285/15	DOLiS/DEC-362/14/28395,28400	Zażalenie na postanowienie WSA w Warszawie z dnia 1.07.2015 r., sygn. akt II SA/Wa 943/15 o odmowie wstrzymania wykonania decyzji w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 1.07.2015 r., sygn. akt II SA/Wa 943/15
117.	15.10.2015 r. I OZ 1247/15	DOLiS/DEC-658/14/13405,13408	Zażalenie na postanowienie WSA w Warszawie z dnia 28.05.2015 r., sygn. akt II SA/Wa 580/15 o wstrzymaniu wykonania decyzji w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 28.05.2015 r., sygn. akt II SA/Wa 580/15
118.	19.10.2015 r. II SA/Wa 86/15	DOLiS/DEC-1093/13/90255,90262	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji
119.	20.10.2015 r. II SA/Wa 1363/15	DOLiS/DEC-367/14/47794,47799	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
120.	21.10.2015 r. II SA/Wa 2138/14	DOLiS/DEC-150/11/76261,76276	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
121.	22.10.2015 r. II SA/Wa 1303/15	DOLiS/DEC-1517/13/48903,48909	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
122.	22.10.2015 r. II SAB/Wa 325/15	DOLiS-440-794/14	Skarga na bezczynność organu w sprawie, dotyczącej braku uaktualnienia danych osobowych	Wyrok WSA stwierdzający, iż bezczynność miała miejsce z rażącym naruszeniem prawa i umarzający postępowanie w

				pozostałym zakresie
123.	22.10.2015 r. II SA/Wa 1532/15	DOLiS/DEC-1274/14/63344,63376	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Postanowienie WSA – odrzucenie skargi
124.	23.10.2015 r. II SA/Wa 117/15	DOLiS/POST-1424/14/89815	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Wyrok WSA – oddalenie skargi
125.	23.10.2015 r. I OZ 1343/15	DOLiS/DEC-1530/12/5458,5463	Zażalenie na postanowienie WSA w Warszawie z dnia 10.06.2015 r. sygn. akt II SA/Wa 475/14 odrzucające skargę kasacyjną od wyroku WSA w Warszawie z dnia 12.12.2014 r., sygn. akt II SA/Wa 475/14 w sprawie ze skargi na decyzję w przedmiocie umorzenia postępowania w sprawie przetwarzania danych osobowych i niespełnienia obowiązku informacyjnego	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia 10.06.2015 r. sygn. akt II SA/Wa 475/14
126.	26.10.2015 r. II SA/Wa 1216/15	DOLiS/DEC-165/12/69181,69183	Skarga na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok WSA – uchylenie zaskarżonej decyzji oraz poprzedzającej ją decyzji
127.	27.10.2015 r. II SA/Wa 1622/15	DOLiS/DEC-1395/14/62555,62570	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
128.	27.10.2015 r. II SA/Wa 1304/15	DOLiS-440-1024/10	Skarga na bezczynność organu w związku z niewykonaniem wyroku WSA w Warszawie z dnia 5.12.2012 r., sygn. akt II SA/Wa 1145/12	Postanowienie WSA - umorzenie postępowania z art. 161 Ppsa
129.	27.10.2015 r. II SAB/Wa 725/15	DOLiS-440-794/14	Skarga na bezczynność organu w sprawie, dotyczącej nie wypełnienia obowiązku informacyjnego	Wyrok WSA - zobowiązujący GIODO do rozpatrzenia zażalenia na nie udzielenie informacji w terminie 14 dni od daty doręczenia prawomocnego wyroku wraz z aktami sprawy i stwierdzający, że bezczynność miała miejsce z rażącym naruszeniem prawa
130.	28.10.2015 r. II SA/Wa 486/15	DOLiS/POST-1093/13/6106,6111	Skarga na postanowienie odmawiające uwzględnienia wniosku o wyjaśnienie wątpliwości dotyczących decyzji	Wyrok WSA – uchylenie zaskarżonego postanowienia
131.	28.10.2015 r. II SA/Wa 183/15	DOLiS/DEC-323/13/93669,93676	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji
132.	28.10.2015 r. II SA/Wa 1333/15	DOLiS/DEC-511/15/49517,49521	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
133.	5.11.2015 r. II SAB/Wa 959/15	DOLiS-440-1463/13	Skarga na przewlekłe prowadzenie postępowania w sprawie, dotyczącej przetwarzania danych osobowych	Postanowienie WSA – odrzucenie skargi

134.	5.11.2015 r. II SA/Wa 450/15	DOLiS/DEC-228/13/102751,102756,102761,102765	Skarga na decyzję w przedmiocie umorzenia postępowania w sprawie ze skargi na przetwarzanie danych osobowych	Wyrok WSA – oddalenie skargi
135.	5.11.2015 r. II SAB/Wa 766/15	DOLiS-440-228/13	Skarga na przewlekłe prowadzenie postępowania w sprawie, dotyczącej przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż przewlekłość miała miejsce z rażącym naruszeniem prawa, wymierzający grzywnę w wysokości 1000 zł i umarzający postępowanie w pozostałym zakresie
136.	5.11.2015 r. I OSK 407/14	DOLiS/DEC-1079/11/8319,8320	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 5.09.2013 r. sygn. akt II SA/Wa 735/13 oddalającego skargę na decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 5.09.2013 r. sygn. akt II SA/Wa 735/13
137.	5.11.2015 r. I OSK 193/14	DOLiS/DEC-168/12/74334,74336	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 8.10.2013 r., sygn. akt II SA/Wa 254/13 uchylającego decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 8.10.2013 r., sygn. akt II SA/Wa 254/13 i oddalający skargę
138.	10.11.2015 r. I OSK 1862/14	DOLiS/DEC-385/12/23990,23992,23994,23995,23997,23999	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 5.12.2013 r. sygn. akt II SA/Wa 1135/13 oddalającego skargę na decyzję w przedmiocie nie uwzględnienia wniosku w sprawie dotyczącej przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 5.12.2013 r. sygn. akt II SA/Wa 1135/13
139.	10.11.2015 r. I OSK 685/14	DOLiS/DEC-74/12/3763,3766,3773	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 25.10.2013 r. sygn. akt II SA/Wa 605/13 uchylającego decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 25.10.2013 r. sygn. akt II SA/Wa 605/13 i oddalający skargę
140.	10.11.2015 r. I OSK 3170/14	DOLiS/DEC-819/12/75909,75916	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 26.06.2014 r. sygn. akt II SA/Wa 2394/14 oddalającego skargę na decyzję w przedmiocie nie uwzględnienia wniosku w sprawie dotyczącej przetwarzania danych osobowych	Wyrok NSA – sprostowanie z urzędu w sentencji wyroku WSA w Warszawie z dnia 26.06.2014 r. sygn. akt II SA/Wa 2394/14 niedokładności oznaczenia przedmiotu sprawy i oddalający skargę kasacyjną
141.	10.11.2015 r. I OSK 1318/14	DOLiS/DEC-384/12/57589,57593,57596,57622	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 19.02.2014 r. sygn. akt II SA/Wa 1945/13 oddalającego skargę na decyzję w przedmiocie nie uwzględnienia wniosku w sprawie dotyczącej udostępnienia	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 19.02.2014 r. sygn. akt II SA/Wa 1945/13

			danych osobowych	
142.	10.11.2015 r. I OSK 1173/14	DOLiS/DEC-434/12/20434,20436	Skargi kasacyjne (w tym GIODO) od wyroku WSA w Warszawie z dnia 15.01.2014 r. sygn. akt II SA/Wa 1082/13 uchylającego w części decyzję w przedmiocie nakazu udostępnienia danych osobowych	Wyrok NSA – oddalenie skarg kasacyjnych od wyroku WSA w Warszawie z dnia 15.01.2014 r. sygn. akt II SA/Wa 1082/13
143.	12.11.2015 r. II SA/Wa 942/15	DOLiS/DEC-974/14/26357,26361	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji
144.	12.11.2015 r. I OSK 566/14	DOLiS/DEC-853/11/26847, 26859,26861	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 8.11.2013 r. sygn. akt II SA/Wa 1264/13 oddalającego skargę na decyzję w przedmiocie nakazu usunięcia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 8.11.2013 r. sygn. akt II SA/Wa 1264/13
145.	12.11.2015 r. II SA/Wa 1780/15	DOLiS/DEC-814/14/74198,74202,74207	Skarga na decyzję w przedmiocie nakazu zaprzestania przetwarzania danych osobowych	Postanowienie WSA – odmowa wstrzymania wykonania zaskarżonej decyzji
146.	12.11.2015 r. I OSK 1242/14	DOLiS/DEC-1049/11/29452,29456	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 28.01.2014 r. sygn. akt II SA/Wa 1366/13 uchylającego decyzję w przedmiocie nakazu usunięcia danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej GIODO od wyroku WSA w Warszawie z dnia 28.01.2014 r. sygn. akt II SA/Wa 1366/13
147.	13.11.2015 r. II SAB/Wa 805/15	DOLiS-440-912/13	Skarga na przewlekłe prowadzenie postępowania w sprawie, dotyczącej odmowy udostępnienia i przetwarzania danych osobowych	Wyrok WSA stwierdzający, iż przewlekłość miała miejsce z rażącym naruszeniem prawa i umarzający postępowanie w pozostałym zakresie
148.	17.11.2015 r. II SA/Wa 761/15	DOLiS/DEC-747/14/10746,10752	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez spełnienie obowiązku informacyjnego oraz odmawiającą uwzględnienia wniosku w przedmiocie usunięcia danych osobowych	Wyrok WSA – oddalenie skargi
149.	19.11.2015 r. II SAB/Wa 537/15	DOLiS-440-450/14	Skarga na bezczynność organu w sprawie, dotyczącej udostępnienia danych osobowych	Wyrok WSA stwierdzający, iż bezczynność miała miejsce z rażącym naruszeniem prawa i umarzający postępowanie w pozostałym zakresie
150.	23.11.2015 r. II SA/Wa 1653/15	DOLiS/DEC-2288/14/78191,78193	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
151.	24.11.2015 r. II SA/Wa 193/15	DOLiS/POST-788/13/92738	Skarga na postanowienie w przedmiocie zwrotu wniosku z tytułu nieuiszczenia opłaty skarbowej	Wyrok WSA – oddalenie skargi
152.	24.11.2015 r. II SA/Wa 1154/15	DOLiS/DEC-1186/13/39661,39665	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji

			uaktualnienie danych osobowych	
153.	24.11.2015 r. II SA/Wa 324/15	DOLiS/DEC-1001/14/1567,1573	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji
154.	24.11.2015 r. I OZ 1534/15	DOLiS-440-831/15	Zażalenie na postanowienie WSA w Warszawie z dnia 23.09.2015 r., sygn. akt II SA/Wa 1402/15 o odmowie przyznania prawa pomocy w sprawie ze skargi na pismo stanowiące odpowiedź na wezwanie do usunięcia naruszenia prawa w przedmiocie skargi dotyczącej nakazania udostępnienia danych osobowych	Postanowienie NSA o oddaleniu zażalenia na postanowienie WSA w Warszawie z dnia
155.	27.11.2015 r. II SA/Wa 1036/15	DOLiS/DEC-614/13/32012,32026	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi, dotyczącej nakazu udostępnienie wniosku	Wyrok WSA- uchylenie zaskarżonej decyzji
156.	2.12.2015 r. II SA/Wa 545/15	DOLiS/DEC-90/13/7191,7193	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji
157.	2.12.2015 r. II SA/Wa 1334/15	DOLiS/DEC-513/15/49565,49569	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji
158.	2.12.2015 r. I OSK 2508/14	DOLiS/DEC-1046/09/3779,3818,3824	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 7.05.2014 r. sygn. akt II SA/Wa 375/14 oddalającego skargę na decyzję w przedmiocie odmowy uwzględnienia skargi na przetwarzanie danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 7.05.2014 r. sygn. akt II SA/Wa 375/14
159.	2.12.2015 r. I OSK 703/14	DOLiS/DEC-25/11/39478,39479,39480	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 6.11.2013 r. sygn. akt II SA/Wa 1590/12 oddalającego skargę na decyzję w przedmiocie odmowy uwzględnienia skargi na przetwarzanie danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 6.11.2013 r. sygn. akt II SA/Wa 1590/12, zaskarżoną decyzję i poprzedzającą ją decyzję
160.	02.12.2015 r. I OSK 2302/14	DIS/DEC-1190/13/76126	Niedopełnienie obowiązku informacyjnego.	umorzenie postępowania kasacyjnego
161.	3.12.2015 r. I OSK 3103/14	DOLiS/DEC-370/12/73257,73259,73260	Skarga kasacyjna na postanowienie WSA w Warszawie z dnia 3.06.2015 r. sygn. akt II SA/Wa 1950/14 o odrzuceniu skargi na decyzję w przedmiocie nakazu usunięcia danych osobowych	Postanowienie NSA – oddalenie skargi kasacyjnej od postanowienia WSA w Warszawie z dnia 3.06.2015 r. sygn. akt II SA/Wa 1950/14
162.	4.12.2015 r. I OSK 945/14	DOLiS/DEC-466/12/5890,5901	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 12.12.2013 r. sygn. akt II SA/Wa 814/13 uchylającego decyzję w przedmiocie odmowy	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 12.12.2013 r. sygn. akt II SA/Wa 814/13 i oddalający skargę

			uwzględnienia wniosku na udostępnienie danych osobowych	
163.	4.12.2015 r. I OSK 599/14	DOLiS/DEC-319/11/55801,55802,55803,55804	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 15.05.2013 r. sygn. akt II SA/Wa 2063/12 oddalającego skargę na decyzję w przedmiocie nie uwzględnienia skargi, dotyczącej przetwarzania danych osobowych	Wyrok NSA – oddalenie skargi kasacyjnej od wyroku WSA w Warszawie z dnia 15.05.2013 r. sygn. akt II SA/Wa 2063/12
164.	4.12.2015 r. I OSK 791/14	DOLiS/DEC-1028/12/31978,31983,31989,31002	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 18.12.2013 r. sygn. akt II SA/Wa 1449/13 uchylającego decyzję w przedmiocie nie uwzględnienia skargi, dotyczącej przetwarzania danych osobowych	Wyrok NSA - uchylający wyrok WSA w Warszawie z dnia 18.12.2013 r. sygn. akt II SA/Wa 1449/13 i przekazujący sprawę do ponownego rozpatrzenia
165.	04.12.2015 r. I OSK 3240/15	DIS/DEC-964/14/77489	Udostępnianie danych osobowych innemu podmiotowi bez podstawy prawnej, pozyskiwanie danych osobowych bez podstawy prawnej.	odmowa wstrzymania wykonania decyzji
166.	04.12.2015 r. I OSK 3192/15	DIS/DEC-1025/14/84758	Udostępnianie danych osobowych innemu podmiotowi bez podstawy prawnej.	odmowa wstrzymania wykonania decyzji
167.	9.12.2015 r. I OSK 1393/14	DOLiS/DEC-212/11/13267, 13270, 13271	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 8.01.2014 r. sygn. akt II SA/Wa 935/13 oddalającego skargę na decyzję w przedmiocie nie uwzględnienia skargi, dotyczącej udostępnienia danych osobowych	Wyrok NSA - oddalający skargę kasacyjną od wyroku WSA w Warszawie z dnia 8.01.2014 r. sygn. akt II SA/Wa 935/13
168.	9.12.2015 r. I OSK 2713/14	DOLiS/DEC-581/10/45756,45759	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 22.05.2014 r. sygn. akt II SA/Wa 507/14 oddalającego skargę na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - uchylający wyrok WSA w Warszawie z dnia 22.05.2014 r. sygn. akt II SA/Wa 507/14 oraz zaskarżoną decyzję.
169.	9.12.2015 r. I OSK 1850/14	DOLiS/DEC-1117/12/38688,38692	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 10.04.2014 r. sygn. akt II SA/Wa 1401/13 oddalającego skargę na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - oddalający skargę kasacyjną od wyroku WSA w Warszawie z dnia 10.04.2014 r. sygn. akt II SA/Wa 1401/13
170.	10.12.2015 r. I OSK 2265/14	DOLiS/DEC-865/12/51163, 51166	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 17.03.2014 r. sygn. akt II SA/Wa 1338/13 oddalającego skargę na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - oddalający skargę kasacyjną od wyroku WSA w Warszawie z dnia 17.03.2014 r. sygn. akt II SA/Wa 1338/13
171.	10.12.2015 r. I OSK 3053/14	DOLiS/DEC-1084/10/901,906	Skarga kasacyjna od wyroku WSA w Warszawie z dnia	Wyrok NSA - oddalający skargę kasacyjną od wyroku WSA w

			2.07.2014 r. sygn. akt II SA/Wa 749/14 oddalającego skargę na decyzję w przedmiocie udzielenia obowiązku informacyjnego odnośnie przetwarzania danych osobowych	Warszawie z dnia 2.07.2014 r. sygn. akt II SA/Wa 749/14
172.	10.12.2015 r. I OSK 1284/14	DOLiS/DEC-667/12/9453,9462, 9467	Skargi kasacyjne (w tym GIODO) od wyroku WSA w Warszawie z dnia 3.12.2013 r. sygn. akt II SA/Wa 747/13 uchylającego decyzję w przedmiocie udostępnienia danych osobowych	Wyrok NSA - oddalający skargi kasacyjne od wyroku WSA w Warszawie z dnia 3.12.2013 r. sygn. akt II SA/Wa 747/13
173.	10.12.2015 r. I OSK 1613/14	DOLiS/POST-221/13/63537	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 24.02.2014 r. sygn. akt II SA/Wa 2249/13 , w sprawie ze skargi na postanowienie w przedmiocie odmowy wszczęcia postępowania w sprawie przetwarzania danych osobowych	Wyrok NSA - uchylający wyrok WSA w Warszawie z dnia 24.02.2014 r. sygn. akt II SA/Wa 2249/13 i oddalający skargę
174.	11.12.2015 r. II SAB/Wa 705/15	DOLiS-440-363/12	Skarga na przewlekłe prowadzenie postępowania w sprawie, dotyczącej wniosku o ponowne rozpatrzenie sprawy w sprawie skargi na przetwarzania danych osobowych	Wyrok WSA zobowiązujący do rozpatrzenia wniosku w terminie 30 dni od daty doręczenia prawomocnego wyroku wraz z aktami sprawy i stwierdzający, że przewlekłość miała miejsce z rażącym naruszeniem prawa
175.	14.12.2015 r. II SAB/Wa 706/15	DOLiS-440-211/14	Skarga na bezczynność i przewlekłe prowadzenie postępowania w sprawie na nieuaktualnienie danych osobowych	Wyrok WSA stwierdzający, że przewlekłość miała miejsce z rażącym naruszeniem prawa, wymierzający grzywnę w wysokości 1000 złotych i umarzający postępowanie w pozostałym zakresie
176.	15.12.2015 r. II SA/Wa 762/15	DOLiS/DEC-1134/12/15384,15390,15402	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie ze skargi na nieprawidłowości w procesie przetwarzania danych osobowych	Wyrok WSA – oddalenie skargi
177.	15.12.2015 r. I OSK 1069/15	DOLiS-440-1188/13	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 9.10.2014 r. sygn. akt II SAB/Wa 411/14 stwierdzającego, że przewlekłość organu miała miejsce z rażącym naruszeniem prawa i wymierzającego GIODO grzywnę w wysokości 2000 zł w sprawie dotyczącej przetwarzania danych osobowych	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 9.10.2014 r. sygn. akt II SAB/Wa 411/14 w części wymierzającej GIODO grzywnę w wysokości 2000 zł i w tym zakresie przekazujący sprawę do ponownego rozpatrzenia oraz oddalający skargę kasacyjną GIODO w pozostałym zakresie
178.	15.12.2015 r. I OSK 1033/15	DOLiS-440-931/12	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 12.11.2014 r. sygn. akt II SAB/Wa 32/14 stwierdzającego,	Wyrok NSA uchylający wyrok WSA w Warszawie z dnia 12.11.2014 r. sygn. akt II SAB/Wa 32/14 w zakresie stwierdzenia, że

			że przewlekłość organu nie miała miejsca z rażącym naruszeniem prawa i umarzającego postępowanie w pozostałym zakresie	przewlekłość organu nie miała miejsca z rażącym naruszeniem prawa i przekazujący w tym zakresie sprawę do ponownego rozpatrzenia.
179.	16.12.2015 r. II SAB/Wa 1131/14	DOLiS-440-394/10	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA stwierdzający, że przewlekłość miała miejsce z rażącym naruszeniem prawa
180.	16.12.2015 r. II SA/Wa 658/15	DIS/DEC-71/15/8533	Przetwarzanie danych biometrycznych bez podstawy prawnej.	oddalenie skargi
181.	18.12.2015 r. II SA/Wa 1800/15	DOLiS/DEC-831/13/75997,76000	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Postanowienie WSA – wstrzymanie wykonania zaskarżonej decyzji
182.	18.12.2015 r. II SA/Wa 580/15	DOLiS/DEC-160/15/13405,13408	Skarga na decyzję w przedmiocie przetwarzania osobowych	Wyrok WSA- uchylenie zaskarżonej decyzji i poprzedzającej jej decyzji

Załącznik nr 4

Informacje przekazane przez organy ścigania w sprawach zawiadomień o popełnieniu przestępstwa skierowanych przez Generalnego Inspektora Ochrony Danych Osobowych w 2015 r.

Informacja	**Rok 2013**	**Rok 2014**	**Rok 2015**
Umorzenie dochodzenia	5	1	5
Umorzenie dochodzenia w części	-	-	-
Umorzenie dochodzenia i podjęcie go na nowo na skutek interwencji Generalnego Inspektora	-	-	-
Umorzenie dochodzenia i odmowa podjęcia go na nowo	-	-	-
Wszczęcie dochodzenia	2	3	6
Odmowa wszczęcia dochodzenia	3	2	5
Wszczęcie śledztwa i jego umorzenie	2	-	-
Postępowanie sprawdzające			1
Zawieszenie dochodzenia	-	-	-
Skierowanie sprawy do sądu	-	-	-
Skazania oraz postanowienia o warunkowym umorzeniu postępowania	-	-	-
Brak informacji	4	4	7

Załącznik nr 5

Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych w 2015 r.

1. II Śląski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 26-27 listopada 2015 r.
2. Międzynarodowa Konferencja i Wystawa „CYBER SECURITY – BEZPIECZEŃSTWO PONAD GRANICAMI". Organizator: Zarząd Targów Warszawskich S.A., 26 listopada 2015 r.
3. Międzynarodowa Konferencja Prawa Własności Intelektualnej i Prawa Nowych Technologii pt. „Value of Information: Intellectual Property, Privacy and Big Data". Organizatorzy: Centrum Prawa Własności Intelektualnej Wydziału Prawa i Administracji Uniwersytetu Gdańskiego we współpracy z amerykańską uczelnią prawniczą Chicago – Kent College of Law. Gdańsk, 20 listopada 2015 r.
4. IV Lubelski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 5-6 listopada 2015 r.
5. V Lubuski Konwent Informatyków i Administracji. Organizator: Szczeciński Park Naukowo-Technologiczny, 5-6 listopada 2015 r.
6. IV edycja Konwentu Ochrony Danych Osobowych i Informacji. Organizatorzy: ForSafe Sp. z o.o. oraz Lubasz i Wspólnicy Kancelaria Radców Prawnych. Łódź, Łódzka Specjalna Strefa Ekonomiczna, 5 listopada 2015 r.
7. II Ogólnopolska Konferencja „Bezpieczeństwo Informacyjne w Szkole". Organizator: Polski Komitet Normalizacyjny. Warszawa, 29 października 2015 r.
8. Konferencja dla dyrektorów szkół zawodowych i Centrów Kształcenia Praktycznego. Organizatorzy: EduFakty – Uczę Nowocześnie, Łódzkie Centrum Doskonalenia Nauczycieli i Kształcenia Praktycznego oraz Zespół Szkół Technicznych w Radomiu. Zgierz, 28-29 października 2015 r.
9. Debata pt. „Relacja ustawy o świadczeniu usług drogą elektroniczną, prawa telekomunikacyjnego oraz ustawy o ochronie danych osobowych. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 27 października 2015 r.
10. IV Wielkopolski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 22-23 października 2015 r.
11. II Podkarpacki Konwent Informatyków i Administracji. Organizator: Szczeciński Park Naukowo-Technologiczny, 15-16 października 2015 r.
12. I Małopolski Konwent Informatyków i Administracji. Organizator: Szczeciński Park Naukowo-Technologiczny. Wieliczka, 8-9 października 2015 r.

13. IX Zachodniopomorski Konwent Informatyków i Administracji. Organizator: Szczeciński Park Naukowo-Technologiczny. Dwór Pomorski, 24-25 września 2015 r.
14. IV Pomorski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 24-25 września 2015 r.
15. I Lubelski Konwent Informatyków i Administracji. Organizator: Szczeciński Park Naukowo-Technologiczny. Lublin, 17-18 września 2015 r.
16. Konferencja „SECURITY CASE STUDY". Organizator: Fundacja Bezpieczna Cyberprzestrzeń. Warszawa, 15-16 września 2015 r.
17. Konferencja Naukowa „Wrześniowe Spotkania z Prawem Pracy". Organizator: Katedra Prawa Pracy Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Spała, 11-13 września 2015 r.
18. VIII Konwent Informatyków i Administracji Pomorza i Kujaw. Organizator: Szczeciński Park Naukowo-Technologiczny. Ciechocinek, 18-19 czerwca 2015 r.
19. V Śląski Konwent Informatyków i Administracji. Organizator: Szczeciński Park Naukowo-Technologiczny. Szczyrk, 11-12 czerwca 2015 r.
20. Mazowiecki Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 28-29 maja 2015 r.
21. „Girls do IT". Organizator: Szkoła Główna Handlowa. Warszawa, 14-15 maja 2015 r.
22. Ogólnopolska Konferencja „Reforma ochrony danych osobowych – nowe szanse i wyzwania". Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją, działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 14 maja 2015 r.
23. Światowy Dzień Społeczeństwa Informacyjnego. Organizator: Polskie Towarzystwo Informatyczne, 14 maja 2015 r.
24. IX Kongres Business Intelligence. Organizator: Bonnier Business Polska, Sp. z o. o. 6-7 maja 2015 r.
25. II Forum IT dla Kierowników w Administracji. Organizator: redakcja miesięcznika „IT w Administracji". Zakopane, 22-24 kwietnia 2015 r.
26. V Dolnośląski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 16-17 kwietnia 2015 r.
27. I Ogólnopolski Kongres Zarządzania Ciągłością Działania. Organizator: SuccessPoint Sp. z o. o. Warszawa 27 marca 2015 r.
28. IV Warmińsko-Mazurski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 26-27 marca 2015 r.
29. XV Sympozjum Świata Telekomunikacji i Mediów. Organizator: Grupa MMC Polska, Warszawa, 25 marca 2015 r.
30. V Konferencja Naukowa „Ataki Sieciowe 2015". Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii działające na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu. Toruń, 24 marca 2015 r.
31. Konferencja „Dyrektor XXI wieku – mobilność, bezpieczeństwo, innowacyjność". Organizator: Librus Sp. z o. o. 23-24 marca 2015 r.
32. IV Małopolski Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji", 12-13 marca 2015 r.

33. IV Łódzki Konwent Informatyków. Organizator: redakcja miesięcznika „IT w Administracji”, 26-27 lutego 2015 r.
34. I Smart City Forum. Organizator: MMC Polska. Warszawa, Hotel Westin, 18-19 lutego 2015 r.

Załącznik nr 6

Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2015 r. w Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty

l.p.	Data	Konferencja/Seminarium	Miejsce
1.	28.01.201	IX Dzień Ochrony Danych Osobowych. Konferencja pt. „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne. Organizator: Generalny Inspektor Ochrony Danych Osobowych.	Warszawa
2.	26.01.2015	Spotkanie z posłami PE nt. zagadnień ochrony danych osobowych w UE. Organizatorzy: Fundacja Panoptykon we współpracy z Biurem Informacyjnym PE.	Warszawa
3.	12.02.2015	Spotkanie pn. „Transfery danych osobowych poza Europejski Obszar Gospodarczy”. Organizator: Grupa Robocza ds. Telekomunikacji, Mediów i Technologii działająca w ramach Brytyjsko-Polskiej Izby Handlowej (BPCC).	Warszawa
4.	12-13.02.2015	Konferencja „Technologie ICT w bankach spółdzielczych”. Organizator: Multiexpo.	Warszawa
5.	9.03.2015	Spotkanie z członkami Regionalnej Izby Gospodarczej w Katowicach. Organizator: Regionalna Izba Gospodarcza w Katowicach.	Katowice
6.	24.03.2015	V Międzynarodowa Konferencja Naukowa „Ataki Sieciowe 2015”. Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii działające na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu.	Toruń
7.	7.05.2015	IX Kongres Business Intelligence. Organizatorzy: Bonnier Business Polska Sp. z o.o., Puls Biznesu.	Warszawa
8.	13.05.2015	II Ogólnopolska Konferencja „ITH – IT w Zdrowiu. Polskie zdrowie w przededniu elektronicznej dokumentacji medycznej”. Organizator: Śląska Sieć Metropolitarna.	Katowice
9.	13.05.2015	XVI Konferencja Okrągłego Stołu – Polska w drodze do Społeczeństwa Informacyjnego. Organizator: Stowarzyszenie Elektryków Polskich.	Warszawa
10.	13-14.05.2015	Konferencja „Girds do IT”. Organizator: Szkoła Główna Handlowa.	Warszawa
11.	14.05.2015	Ogólnopolska Konferencja „Reforma ochrony danych osobowych – nowe szanse i wyzwania”. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
12.	15.05.2015	VII Konferencja Naukowa „Bezpieczeństwo w Internecie. Internet Rzeczy. Bezpieczeństwo Smart City”. Organizator: Uniwersytet Kardynała Stefana Wyszyńskiego.	Warszawa
13.	18.05.2015	Konferencja Szkoleniowa „Ochrona danych osobowych – obowiązki przedsiębiorców w świetle nowych przepisów prawa od 1 stycznia 2015 roku”. Organizator: Polska Izba Przemysłu Targowego.	Warszawa
14.	21.05.2015	Seminarium podsumowujące Ogólnopolski Program Edukacyjny GIODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana	Częstochowa

		do uczniów i nauczycieli". Organizator: Miejski Ośrodek Kultury w Częstochowie.	
15.	29.09.2015	Seminarium podsumowujące Ogólnopolski Program Edukacyjny GIODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Organizator: Zespół Szkół Samochodowo-Budowlanych w Częstochowie.	Częstochowa
16.	1.06.2016	Konferencja „Standard of personal data protection in the area of police and judicial cooperation in criminal matters in the European Union". Organizator: Szkoła Główna Handlowa w Warszawie.	Warszawa
17.	9.06.2015	Konferencja „Internet jako dobro wspólne". Organizator: Sejm RP, Komisja Administracji i Cyfryzacji.	Warszawa
18.	22.06.2015	Seminarium szkoleniowe dla sekretarzy gmin województwa warmińsko-mazurskiego. Organizator: Klub Sekretarzy Województwa Warmińsko-Mazurskiego.	Olsztyn
19.	10.09.2015	Zjazd pracowników Departamentu Ochrony Centralnego Biura Antykorupcyjnego. Organizator: Centralne Biuro Antykorupcyjne.	Lucień
20.	12.09.2015	Konferencja Naukowa „Wrześniowe spotkania z prawem pracy". Organizator: Katedra Prawa Pracy Wydziału Prawa i Administracji Uniwersytetu Łódzkiego.	Spała
21.	18.09.2015	Konferencja Naukowa „Nowe ramy ochrony danych osobowych w Unii Europejskiej. Wyzwania dla Polski".	Warszawa
22.	24-25.09.2015	XXI Forum Teleinformatyki „Reforma prawa ochrony danych osobowych a przetwarzanie wielkich zasobów danych". Organizator: BizTech Consulting.	Miedzeszyn
23.	29.09.2015	II Ogólnopolska Konferencja „Bezpieczeństwo Informacyjne w Szkole". Organizator: Polski Komitet Normalizacyjny.	Radom
24.	30.09.2015	Warsztaty zarządzania Internetem „Sprawdź kto rządzi Internetem. Internet dzisiaj i jutro". Organizatorzy: Ministerstwo Administracji i Cyfryzacji, Internet Corporation for Assigned Names and Numbers (ICANN), Naukowa i Akademicka Sieć Komputerowa (NASK) oraz Internet Society Poland.	Warszawa
25.	1.10.2015	Europejskie Forum Nowych Idei. Organizator: Konfederacja Lewiatan.	Sopot
26.	2.10.2015	Wykład inauguracyjny z okazji uroczystości rozpoczęcia roku akademickiego 2015/2016 w Wyższej Szkole Policji w Szczytnie.	Szczytno
27.	10.10.2015 r	Wykład inauguracyjny w związku z uroczystością otwarcia pierwszej edycji studiów podyplomowych pt. „Wykonywanie funkcji administratora bezpieczeństwa informacji" organizowanych przez Instytut Nauk Prawnych Polskiej Akademii Nauk (INP PAN) pod patronatem Generalnego Inspektora Ochrony Danych Osobowych.	Warszawa
28.	13.10.2015	Forum Bezpieczeństwa Telekomunikacyjnego - Telecom Security Forum TelSec 2015. Organizator: Orange Polska S.A.	Serock
29.	14.10.2015	V Europejski Kongres MŚP. Organizatorzy: Regionalna Izba Gospodarcza w Katowicach, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego.	Katowice
30.	14.10.2015	Konferencja „Innowacyjność w ochronie informacji biznesowych i danych osobowych szansą na rozwój sektora MŚP". Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.	Katowice
31.	22.10.2015	Konferencja „Działalność służb specjalnych Państwa a ochrona danych osobowych". Organizatorzy: GIODO, CBA i UKSW.	Warszawa

32.	27.10.2015	Debata pt. „Relacja ustawy o świadczeniu usług drogą elektroniczną, prawa telekomunikacyjnego oraz ustawy o ochronie danych osobowych". Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego	Łódź
33.	29.10.2015	II Ogólnopolska Konferencja „Bezpieczeństwo Informacyjne w Szkole". Organizator: Polski Komitet Normalizacyjny.	Warszawa
34.	5.11.2015	IV Konwent Ochrony Danych Osobowych i Informacji. Organizatorzy: ForSafe Sp. z o.o. oraz Lubasz i Wspólnicy Kancelarii Radców Prawnych.	Łódź
35.	23.11.2015	I Krajowe Forum Liderów IT i Bezpieczeństwa Biznesu. Organizator: Vmware we współpracy z Fundacją IT Leader Club Polska.	Warszawa
36.	26.11.2015	III Międzynarodowa Konferencja i Wystawa „Cyber Security – bezpieczeństwo ponad granicami".	Warszawa
37.	26.11.2015	VIII Kongres Bankowości Elektronicznej. Organizator: Górska Akademia Handlowa.	Warszawa
38.	1.12.2015	Dzień Otwarty w Redakcji „IT w Administracji" „Obowiązki ABI po nowelizacji ustawy o ochronie danych osobowych".	Warszawa
39.	10.12.2015	Ogólnopolska Konferencja "Edu IT. Nowe technologie w edukacji". Organizator: magazyn „EduFakty – Uczę Nowocześnie".	Gliwice
40.	16.12.2015	Seminarium e-biznesu „Nowe technologie cyfrowe a modele biznesu". Organizatorzy: Zakład Systemów Zarządzania Szkoły Głównej Handlowej oraz Koło Nowych Technologii Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie.	Warszawa

Załącznik nr 7

Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2015 r. za granicą

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	8.01.2015	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers)	Bruksela
2.	12.01.2015	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
3.	13-14.01.2015	Spotkanie Podgrupy ds. Technologii.	Bruksela
4.	20-21.01.2015	Obchody IX Europejskiego Dnia Ochrony Danych Osobowych.	Bruksela
5.	20.01.2015	I spotkanie partnerów projektu PHAEDRA II.	Bruksela
6.	20-21.01.2015	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
7.	2-4.02.2015	99. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
8.	4.02.2015	Konferencja nt. konsekwencji cywilnego wykorzystania dronów w kontekście ochrony danych osobowych i prywatności. Organizator: węgierski organ ochrony danych osobowych.	Budapeszt
9.	3-5.03.2015	Spotkanie Podgrupy ds. Technologii.	Bruksela
10.	11.03.2015	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
11.	19.03.2015	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers).	Bruksela
12.	24-26.03.2015	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29, Grupy Koordynującej Nadzór nad Systemem Informacyjnym Schengen (SIS II), Grupy Koordynującej Nadzór nad Wizowym Systemem Informacyjnym (VIS) oraz Grupy Koordynującej Nadzór nad systemem EURODAC	Bruksela
13.	13-15.04.2015	100. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
14.	28.04-1.05.2015	Spotkanie Grupy CEEDPA.	Durres
15.	18-20.05.2015	Wiosenna Konferencja Organów Ochrony Danych (European Conference of Data Protection Authorities)	Manchester
16.	19-20.2015	Spotkanie Podgrupy ds. Technologii.	Bruksela
17.	21.05.2015	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
18.	21-22.05.2015	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers) oraz Podgrupy ds. Przyszłości Prywatności (Future of Privacy), Grupy Roboczej Art. 29.	Bruksela
19.	24-29.05.2015	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Ankara
20.	29.05.2015	Posiedzenie Podgrupy ds. Współpracy, Grupy Roboczej Art. 29.	Bruksela
21.	3-4.06.2015	Posiedzenie JSB (Europol) oraz posiedzenie JSA (Customs)	Bruksela
22.	14-19.06.2015	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Londyn
23.	15-17.06.2015	101. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
24.	21-23.06.2015	Konferencja edukacyjna dotycząca wyzwań w ochronie prywatności, z okazji dziesięciolecia macedońskiego organu ochrony danych osobowych. Organizator: macedoński organ ochrony danych osobowych.	Skopje
25.	22-24.06.2015	Warsztaty dotyczące naruszeń ochrony danych.	Ispra
26.	30.06-3.07.2015	32. Posiedzenie Plenarne Komitetu Konsultacyjnego do spraw	Strasburg

		Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD).	
27.	1-3.07.2015	Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela
28.	16.07.2015	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers).	Bruksela
29.	22.07.2015	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
30.	22-23.07.2015	Posiedzenie Podgrupy ds. Współpracy, Grupy Roboczej Art. 29.	Bruksela
31.	3-4.09.2015	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29 oraz Spotkanie Grupy Roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych (Working Party on Information Exchange and Data Protection – DAPIX).	Bruksela
32.	7.09.2015	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
33.	8-9.09.2015	Spotkanie Podgrupy ds. Technologii.	Bruksela
34.	21-23.09.2015	102. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
35.	21-25.09.2015	Spotkanie w sprawie ewaluacji Schengen z zakresu ochrony danych osobowych. Organizatorzy: Komisja Europejska, Urząd Danych Osobowych w Holandii.	Amsterdam
36.	24-25.09.2015	Spotkanie eksperckie w sprawie biometrii w wielkoskalowych systemach IT Unii Europejskiej. Organizator: Agencja praw Podstawowych.	Wiedeń
37.	27-30.09.2015	Warsztaty rozpatrywania spraw	Tirana
38.	7-8.10.2015	Spotkanie grup koordynujących nadzór nad SIS, VIS i Eurodac.	Bruksela
39.	11-12.10.2014	Posiedzenie JSB Europol.	Bruksela
40.	12-14.10.2015	58. posiedzenie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska).	Berlin
41.	18-25.10.2015	Czynności kontrolne Systemu Informacyjnego Schengen (SIS II, VIS).	Tbilisi
42.	25-29.10.2015	37. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności. Organizator: Urząd Danych Osobowych w Holandii.	Amsterdam
43.	3.11.2015	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
44.	9-11.11.2015	The 6th International Personal Data Protection Conference. Organizator: Roskomnadzor Zharov.	Moskwa
45.	17-18.11.2015	4. warsztaty ds. naruszeń ochrony danych. Organizatorzy: Komisja Europejska oraz Joint Research Centre.	Ispra
46.	24-25.11.2015	Warsztat w ramach projektu PHAEDRA (PHAEDRA II Roundtable)	Bruksela
47.	6-11.12.2015	Czynności kontrolne Systemu Informacyjnego Schengen (SIS II, VIS).	Madryt
48.	9-11.12.2015	Posiedzenie: WON Europolu, WON ds. Celnych, Grupy Koordynującej Nadzór nad CIS, Spotkanie przewodniczących i wiceprzewodniczących Grup Koordynujących Nadzór Nad Systemami Wymiany Informacji w UE	Bruksela
49.	16.12.2015	103. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela