Druk nr 2170

Warszawa, 28 grudnia 2017 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Generalny Inspektor Ochrony Danych Osobowych
DESiWM-031-1/17/93427/17

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 2016.

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), 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

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

SPRAWOZDANIE Z DZIAŁALNOŚCI **GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH** W ROKU 2016

Sprawozdanie stanowi wykonanie art. 20 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922), 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.

Sprawozdanie obejmuje okres działalności Generalnego Inspektora Ochrony Danych Osobowych od 1 stycznia 2016 r. do 31 grudnia 2016 r.

Warszawa
2017

SPIS TREŚCI

Szanowni Państwo,

zgodnie z ustawą o ochronie danych osobowych, raz do roku przedkładam Sejmowi RP sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych.

GIODO od niemal 20 lat stoi na straży zgodnego z prawem i bezpiecznego przetwarzania naszych danych osobowych. W świecie dynamicznie rozwijających się nowoczesnych technologii, informacje na nasz temat stają się nieodzownym elementem niemal każdej usługi czy produktu. Nie bez powodu dane osobowe nazywa się ropą naftową XXI w. Z tym większym zaangażowaniem musimy je chronić.

Niniejsze sprawozdanie prezentuje najważniejsze ustalenia i wnioski z realizowanych przez GIODO w 2016 r. ustawowych zadań, wśród których wymienić można rozpatrywanie skarg obywateli, prowadzenie kontroli, opiniowanie projektów aktów prawnych, rejestrowanie zbiorów danych czy też działalność edukacyjną.

Rok 2016, będący rokiem sprawozdawczym niniejszego opracowania, był czasem szczególnym dla systemu ochrony danych osobowych w Polsce i Europie. 27 kwietnia przyjęto bowiem ogólne rozporządzenie o ochronie danych, które – utrzymując dotychczasowe wartości i zasady ochrony danych - w znaczący jednak sposób zmienia podejście do ochrony naszej prywatności. Rozporządzenie, które będziemy stosować od 25 maja 2018 r., stanowi bardzo duże wyzwanie zarówno dla administratorów danych, jak i organu nadzorczego – GIODO. Jednak tylko jego właściwe wdrożenie i stosowanie może przynieść zakładany przez unijnego ustawodawcę efekt – skuteczniejszą ochronę danych osobowych obywateli.

Mam nadzieję, że niniejsze sprawozdanie z działalności GIODO będzie nie tylko rzetelną informacją o działalności polskiego organu ochrony danych, ale również podstawą do podejmowania decyzji służących zwiększeniu poziomu bezpieczeństwa naszych danych osobowych.

dr Edyta Bielak-Jomaa

Generalny Inspektor Ochrony Danych Osobowych

I. Wprowadzenie

1. Źródła prawa w zakresie ochrony danych osobowych

Podstawę prawną działania Generalnego Inspektora Ochrony Danych Osobowych stanowi ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Z 2016 r. poz. 922) oraz wydane na jej podstawie akty wykonawcze:

- 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 i rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 19 listopada 2015 r. Zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. z 2015 r. poz. 2020)
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015 r. poz. 745);
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015 poz. 719);
- 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);
- 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);
- 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. z 2008 r. Nr 229, poz. 1536);
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

Zadania i kompetencje Generalnego Inspektora Ochrony Danych Osobowych wyznaczają

przepisy ustawy o ochronie danych osobowych. W ich świetle GIODO jest uprawniony do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- zapewnienia wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z wydanych decyzji przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2014 r. poz. 1619 z późn. zm.),
- prowadzenia rejestru zbiorów danych oraz rejestru administratorów bezpieczeństwa informacji, a także udzielania informacji o zarejestrowanych zbiorach danych i zarejestrowanych administratorach bezpieczeństwa informacji,
- opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenia w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

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 czy też decyzji Rady nr 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiającej Europejski Urząd Policji (Europol).** W lipcu 2016 r. weszło 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 ma związek z nowymi zadaniami dla Generalnego Inspektora Ochrony Danych Osobowych. GIODO stał się na mocy tych przepisów organem właściwym do przyjmowania zgłoszeń przypadków naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osoowe.

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 2017 r. poz. 1907 t.j.) 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 zgodnie z opracowaną instrukcję postępowania.

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.

1.1. Nowe prawo Unii Europejskiej w zakresie ochrony danych osobowych.

Parlament Europejski 14 kwietnia 2016 r. przyjął pakiet legislacyjny dotyczący nowych unijnych ram prawnych ochrony danych osobowych, kończąc w ten sposób trwające ponad cztery lata prace nad przebudową unijnych zasad ochrony danych. Reforma unijnego prawa ochrony danych opierała się na dwóch podstawowych zamierzeniach – ujednolicenia przepisów o ochronie o ochronie danych osobowych na terenie UE oraz dostosowania zasad ochrony prywatności do wyzwań technologicznych XXI wieku.

Nowo uchwalone rozporządzenie uchyla obowiązującą dotychczas dyrektywę 95/46/WE, zaś nowa dyrektywa uchyla decyzję ramową Rady 2008/997/WSiSW. Nowe prawo o ochronie danych osobowych ma zapewnić wysoki, ujednolicony poziom ochrony danych w całej Unii Europejskiej, przyczyniając się do wzrostu poczucia pewności prawnej w tym zakresie

Na pakiet składają się z dwa dokumenty, które weszły w życie 24 maja 2016 r. (Dziennik Urzędowy UE L 119):

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane często RODO,
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. 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 oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Najważniejszą zmianą, jaką niesie europejskie prawo o ochronie danych osobowych dla administratorów jest zmiana podejścia do systemu zarządzania ochroną przetwarzanych informacji. Rozporządzenie w większym stopniu przenosi bowiem ciężar odpowiedzialności za przestrzeganie zasad i obowiązków wynikających

z nowych przepisów na administratorów danych osobowych, wprowadzając do systemu ochrony danych podejście oparte na ryzyku, zasadę rozliczalności, obowiązek uwzględniania ochrony danych osobowych w fazie projektowania czy też ocenę skutków dla ochrony danych.

Z perspektywy GIODO, ogólne rozporządzenie jest szalenie istotnym wyzwaniem z uwagi na wiele nowych obowiązków, jakie na organy nadzorcze nakłada ten akt. Wśród nich wymienić można:

- uprawnienie do nakładania administracyjnych kar pieniężnych za naruszenia przepisów o ochronie danych w maksymalnej wysokości nawet 20 mln EURO,
- przyjmowanie zawiadomień o naruszeniu ochrony danych od wszystkich administratorów danych (a nie jak dotychczas jedynie z sektora telekomunikacyjnego),
- opiniowanie, zatwierdzanie, publikowanie i rejestrowanie kodeksów postępowania,
- certyfikacja i akredytacja podmiotów certyfikujących,
- udzielanie pisemnych zaleceń w ramach przeprowadzanych przez administratorów danych ocen skutków dla ochrony danych,
- większa niż dotychczas współpraca z inspektorami ochrony danych (obecnymi administratorami bezpieczeństwa informacji – ABI),
- większy nacisk na prowadzoną przez organ nadzorczy działalność edukacyjną na rzecz podnoszenia świadomości i wiedzy na temat ochrony danych osobowych,
- stworzenie mechanizmu kompleksowej współpracy i mechanizmu spójności na rzecz międzynarodowej współpracy administracyjnej – nowe instrumenty zakładające dużo większe niż dotychczas zaangażowanie GIODO w prowadzenie spraw o charakterze transgranicznym, w tym także udział w tworzonej przepisami rozporządzenia Europejskiej Radzie Ochrony Danych.

Nowe przepisy zawarte w dyrektywie policyjnej mają z kolei na celu ochronę osób w związku z przetwarzaniem danych osobowych na potrzeby zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych.

Ogólne rozporządzenie o ochronie danych weszło w życie już w maju ubiegłego roku, natomiast będzie stosowane od 25 maja 2018 r. Z uwagi na szczególny charakter prawny rozporządzenia, oznaczać to będzie, że wszystkie materialne przepisy tego dokumentu będą od tego dnia obowiązywać bezpośrednio i będą miały bezpośredni skutek. Zatem wszystkie obowiązki administratorów danych będą musiały być wykonywane już od 25 maja 2018 r.

Wtedy też osoby, których dane są przetwarzane będą mogły korzystać z przysługujących im nowych uprawnień, takich jak prawo do przenoszenia danych, czy prawo do bycia zapomnianym.

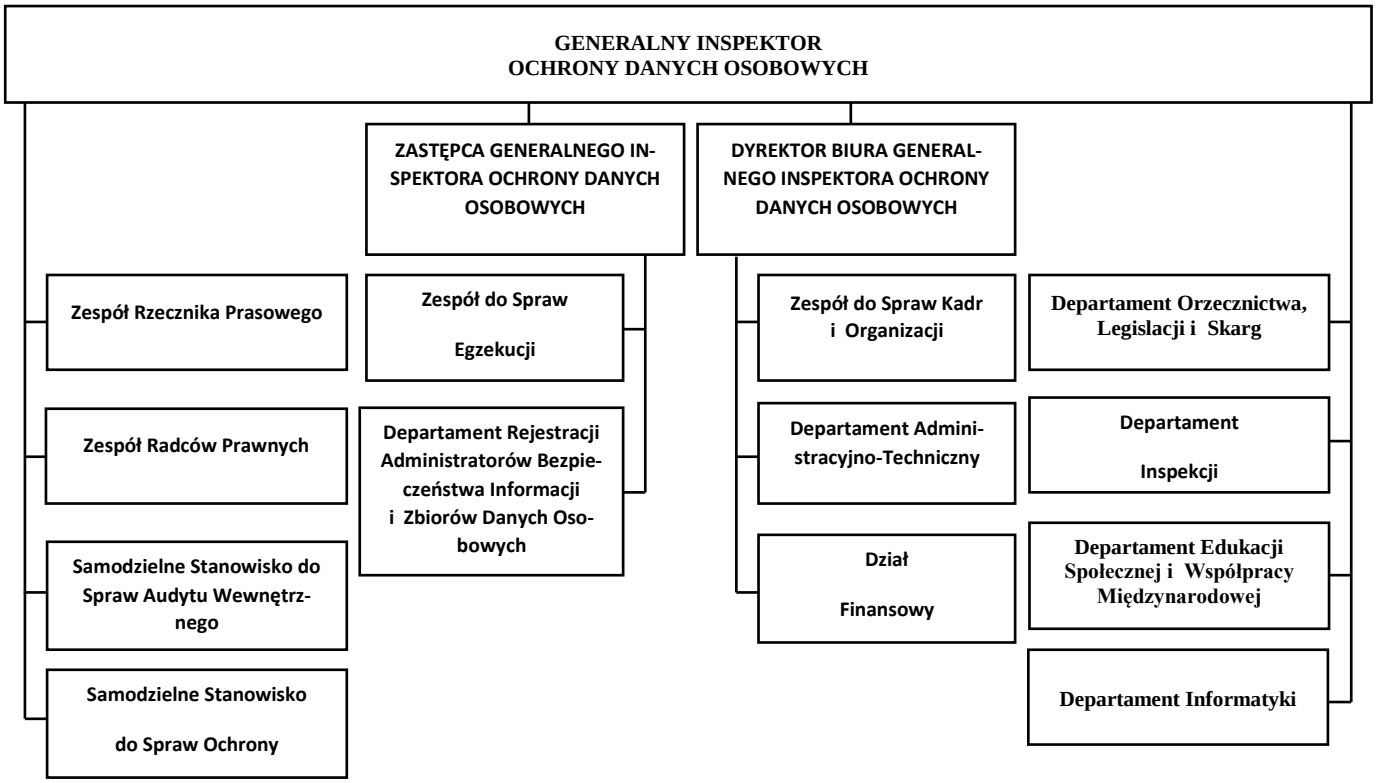
Choć rozporządzenie będzie stosowane bezpośrednio to jednak pozostają obszary, które wymagają działań na poziomie krajowym, np. zmiany przepisów sektorowych – tak by wszystkie akty prawne regulujące przetwarzanie danych osobowych w Polsce były 25 maja 2018 r. zgodne z ogólnym rozporządzeniem o ochronie danych osobowych. W Polsce prace te koordynuje Ministerstwo Cyfryzacji. Podczas tego „okresu przejściowego" państwa członkowskie mają zatem obowiązek dostosowania krajowych przepisów do nowych, zmodernizowanych i uaktualnionych zasad ochrony danych osobowych.

2. Biuro Generalnego Inspektora Ochrony Danych Osobowych

2.1. Struktura organizacyjna

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

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



Wykres 1. ***Struktura organizacyjna Biura Generalnego Inspektora Ochrony Danych Osobowych.***

[1] Zarządzenie nr 5/2016 Generalnego Inspektora Ochrony Danych Osobowych z dnia 30 marca 2016 r. W sprawie wprowadzenia Regulaminu Organizacyjnego Biura Generalnego Inspektora Ochrony Danych Osobowych.

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.

2.2. Pracownicy Biura GIODO

Stan zatrudnienia w Biurze GIODO w przeliczeniu na pełne etaty wynosił na dzień 1 stycznia 2016 r. – 145,73 etatów (tj. 149 osób), zaś na dzień 31 grudnia 2016 r. – 151,525 etatów (tj. 155 osób). Na stanowiskach merytorycznych zatrudnione były 134 osoby, a na stanowiskach pomocniczych 21 osób. Wyższe wykształcenie posiadało 136 pracowników, w tym 99 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na koniec 2016 r. przedstawia się następująco:

- GIODO - 1 osoba (1 etat)

- Zastępca GIODO – 1 osoba (1 etat)[2]

- Dyrektor Biura – 1 osoba (1 etat)

- Zespół Rzecznika Prasowego (ZP) – 6 osób (6 etatów)

- Departament Edukacji Społecznej i Współpracy Międzynarodowej (DESiWM) – 12 osób (11,75 etatu),

- Departament Informatyki (DIF) – 10 osób (9,75 etatu),

- Departament Inspekcji (DIS) – 21 osób (21 etatów),

- Departament Administracyjno-Techniczny (DAT) – 18 osób (17,40 etatu),

- Departament Orzecznictwa, Legislacji i Skarg (DOLiS) – 47 osób (46,125 etatów),

- Departament Rejestracji Administratorów Bezpieczeństwa Informacji i Zbiorów Danych Osobowych (DR) – 22 osoby (22 etaty),

- Dział Finansowy (GK)– 3 osoby (3 etaty),

- Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych (SOIN) – 1 osoba (1 etat),

- Zespół ds. Kadr i Organizacji (ZKO) – 4 osoby (4 etaty),

- Samodzielne Stanowisko ds. Audytu Wewnętrznego (SAW) – 1 osoba (0,5 etatu),

- Zespół Radców Prawnych (ZRP) – 3 osoby (2 etaty),

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

- Radca – samodzielne stanowisko - 1 osoba (1 etat)

[2] Z końcem 2016 r. minister Andrzej Lewiński, po ponad dziesięcioletniej pracy na stanowisku zastępcy GIODO, przeszedł na emeryturę.

2.3. Budżet Generalnego Inspektora Ochrony Danych Osobowych za 2016 r

Budżet Generalnego Inspektora Ochrony Danych Osobowych ustalony w ustawie budżetowej na 2016 r. wynosił: 19 287 tys. Zł., w tym:

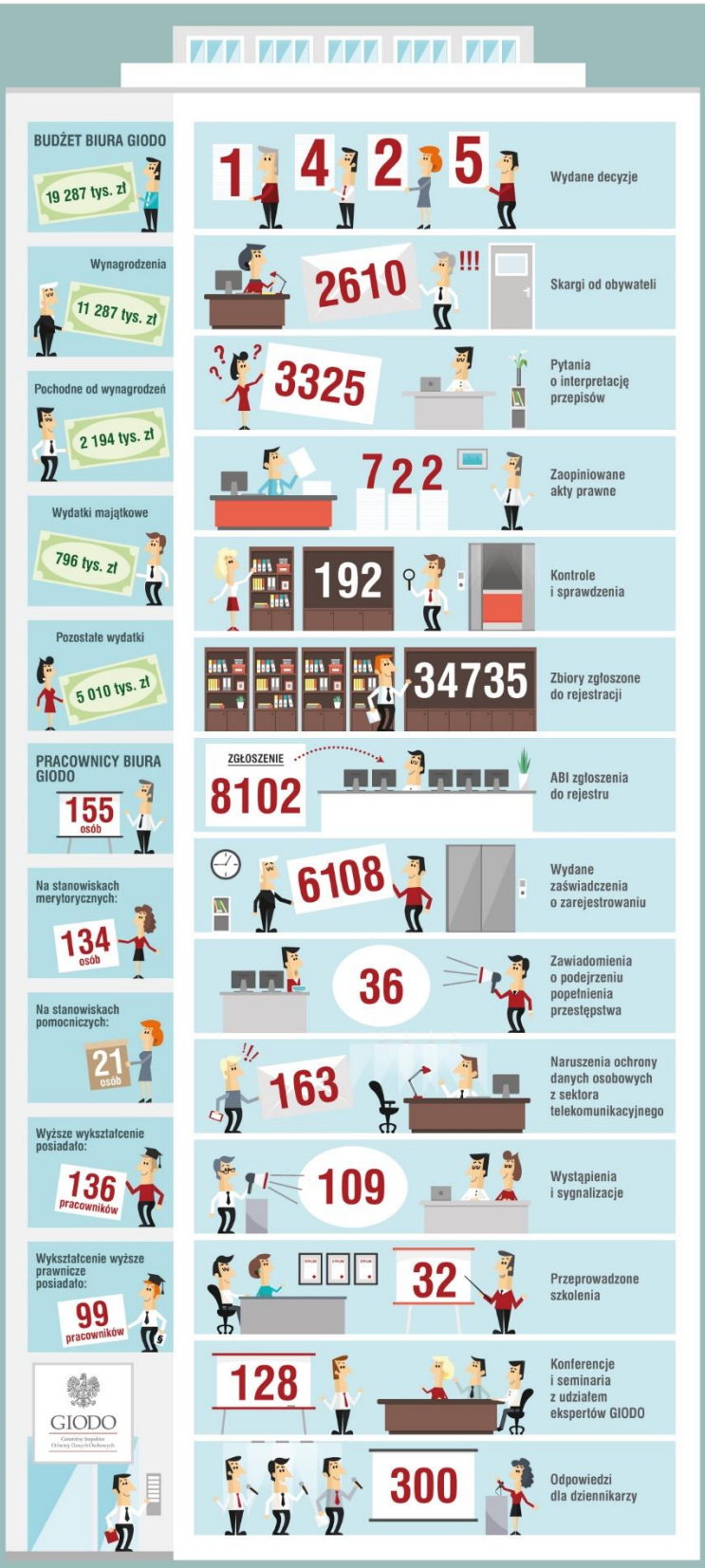
- wynagrodzenia	11 287 tys. zł
- pochodnie od wynagrodzeń	2 194 tys. zł
- wydatki majątkowe	796 tys. zł
- pozostałe wydatki	5 010 tys. zł

Wydatki zrealizowane przez GIODO w 2016 roku w kwocie 18 180 tys. zł obejmowały:

- wynagrodzenia	11 174 tys. zł
- pochodne od wynagrodzeń	1 971 tys. zł
- wydatki majątkowe	460 tys. zł
- pozostałe wydatki	4 575 tys. zł

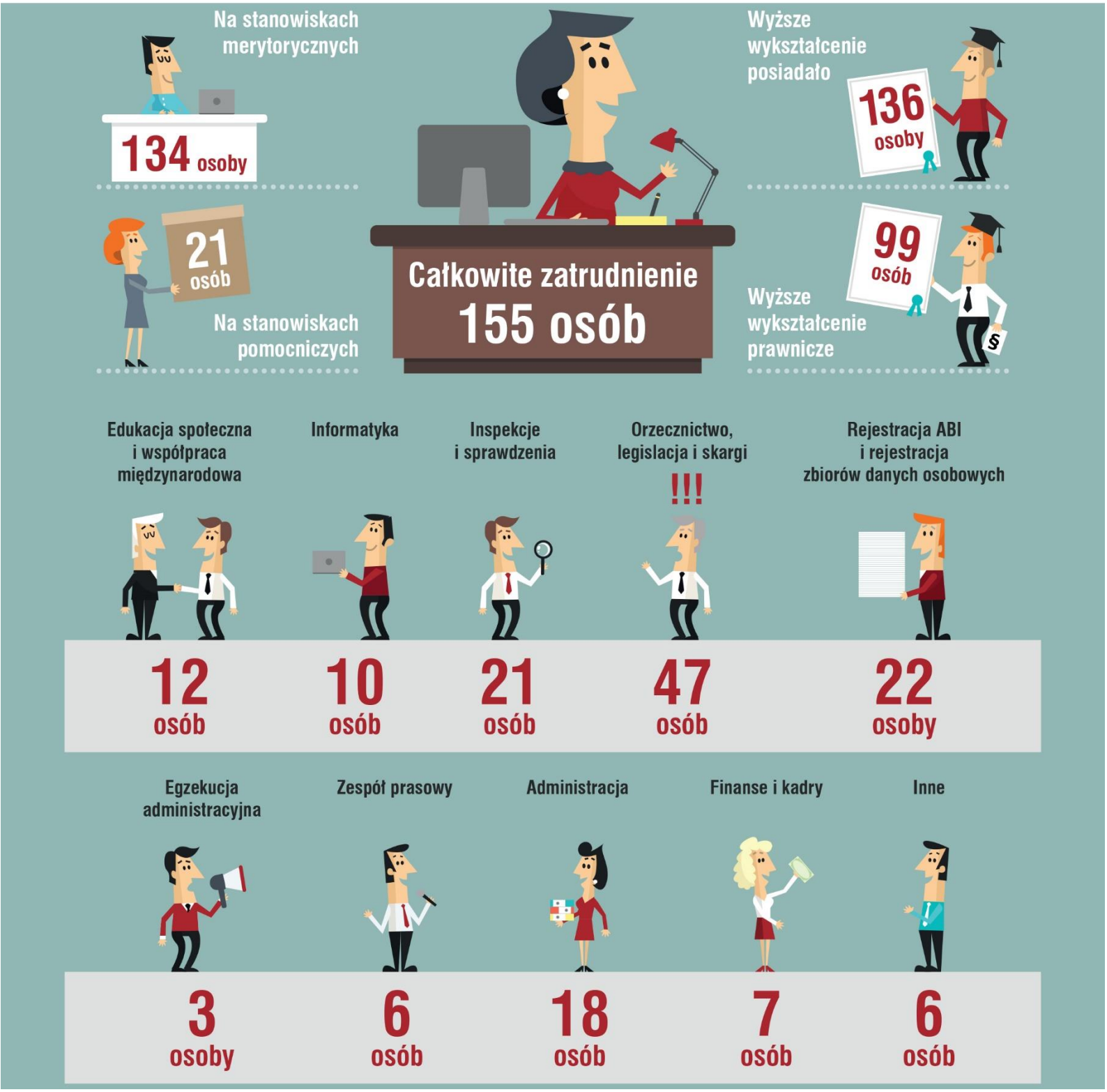
W kontekście wejścia w życie ogólnego rozporządzenia o ochronie danych warto podkreślić, że same przepisy tego aktu wprost wskazują na konieczność zapewnienia organowi nadzorczemu odpowiednich środków finansowych niezbędnych do realizacji zadań i gwarantujących jego niezależność. Jak stanowi art. 52 ust. 4, „każde państwo członkowskie zapewnia, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wypełniania swoich uprawnień(…)". Warto zaznaczyć, że wzmocnienie organów nadzorczych to jedno z głównych założeń reformy przepisów o ochronie danych. Na potrzebę zapewnienia adekwatnych środków zwróciła uwagę również Grupa Robocza Art. 29, przyjmując 4 maja 2017 r. list skierowany do rządów państw członkowskich, w którym potrzebę wzmocnienia organów nadzorczych uzasadniano m.in. „absolutną koniecznością przygotowania i profesjonalnego wdrożenia nowych ram prawnych (…), szkolenia pracowników, aktualizacji systemów informatycznych, propagowania świadomości i zapewniania wytycznych na temat nowych zasad".

GIODO w liczbach / 2016 r.

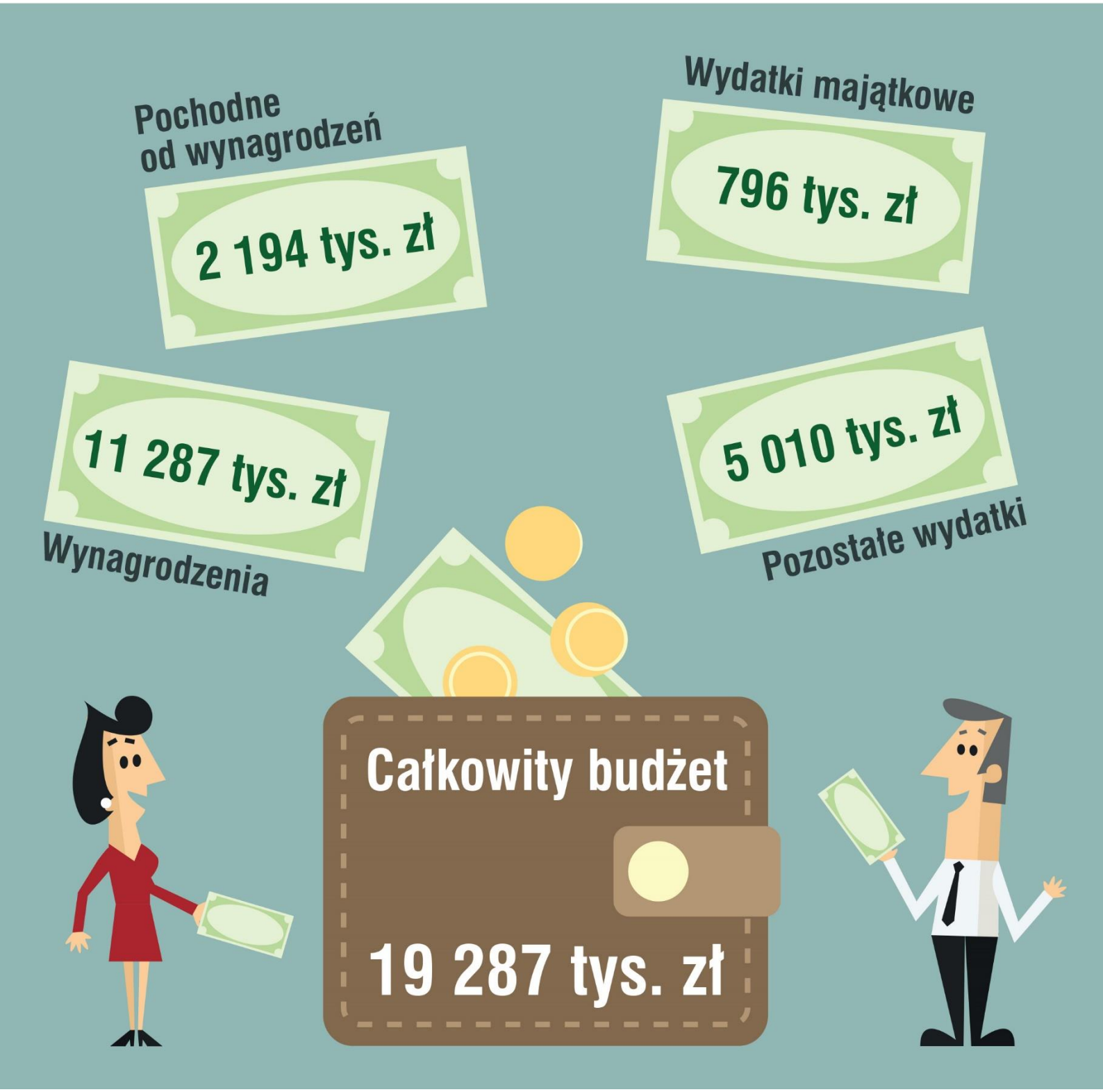


GIODO

GIODO w liczbach / 2016 r.
Pracownicy biura



GIODO w liczbach / 2016 r.
Budżet biura



GIODO

GIODO w liczbach / 2016 r.
Skargi od obywateli

Liczba pracowników zajmujących się rozpatrywaniem skarg

Liczba otrzymanych skarg

Liczba wydanych decyzji przez GIODO

Korespondencja wychodząca w sprawach skarg

Liczba decyzji GIODO zaskarżonych do WSA

GIODO

GIODO w liczbach / 2016 r.
Kontrole

Liczba pracowników zajmujących się kontrolami

Liczba kontroli przeprowadzonych przez GIODO

Liczba wniosków GIODO o dokonanie sprawdzenia przez ABI

Liczba systemów informatycznych skontrolowanych przez GIODO

GIODO w liczbach / 2016 r.

Opiniowanie aktów prawnych i interpretacja przepisów

Opiniowanie aktów prawnych

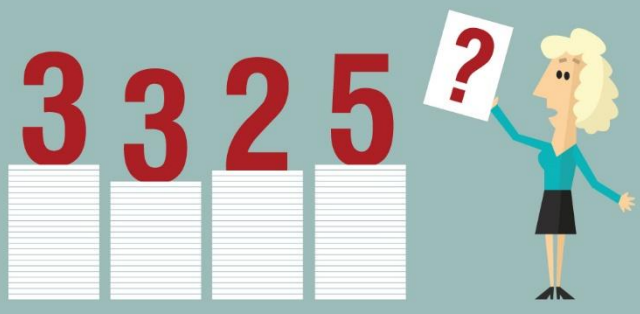
Liczba pracowników zajmujących się legislacją

Liczba zaopiniowanych aktów prawnych

Interpretacja przepisów

Liczba pracowników zajmujących się odpowiedziami na pytania

Liczba pytań z prośbą o interpretację



GIODO

GIODO w liczbach / 2016 r.
Rejestracja zbiorów danych osobowych

Liczba pracowników zajmujących się rejestracją

Liczba zbiorów zgłoszonych do rejestracji

(27844 przy użyciu elektronicznego programu wspomagającego eGIODO)

Liczba zbiorów wpisanych do rejestru

Liczba wydanych decyzji

Liczba pism wychodzących do zgłaszających zbiory

Liczba wydanych zaświadczeń o zarejestrowaniu zbioru

GIODO w liczbach / 2016 r.
Rejestracja administratorów bezpieczeństwa informacji

Liczba pracowników zajmujących się rejestracją ABI

Liczba zgłoszonych powołań ABI

Liczba ABI wpisanych do rejestru

Liczba zgłoszonych odwołań ABI

Liczba wydanych zaświadczeń o zarejestrowaniu ABI

GIODO w liczbach / 2016 r.
Działalność edukacyjno-szkoleniowa

Liczba pracowników zajmujących się edukacją i szkoleniami

Szkolenia GIODO

2016 i 2017
– ponad 1000
przeszkolonych ABI

W sumie w 2016 r.
przeprowadzono
32 szkolenia
podmiotów zewnętrznych

Konferencje i seminaria z udziałem ekspertów GIODO

Liczba patronatów
udzielonych przez GIODO

Program edukacyjny GIODO Twoje Dane - Twoja Sprawa edycja 2016/2017

Zaangażowanych
w realizację Programu

II. Ochrona prywatności obywateli

1. Wprowadzenie

Każdy ma prawo do ochrony dotyczących go danych osobowych. Ustawa o ochronie danych osobowych wprowadza szczegółowe normy służące realizacji tego prawa. Przede wszystkim reguluje postępowanie przy przetwarzaniu danych osobowych, czyli operacjach takich, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Za dane osobowe uważa się wszelkie informacje dotyczące osoby fizycznej, pozwalające bez większego wysiłku na określenie jej tożsamości. 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.

Zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 26 ust. 1 ustawy, ujmując je w formę podstawowych obowiązków administratora danych . 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:

- **legalności** – dane mogą być przetwarzane tylko na podstawie jednej z przesłanek określonych w przepisach prawa ochrony danych,
- **celowości** – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z tymi celami,
- **merytorycznej poprawności** – dane powinny być merytorycznie poprawne,
- **adekwatności** – dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane,
- **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.

Niezmienne wartości systemu ochrony danych osobowych.

RODO nie powstało w próżni. Ponad 20 lat doświadczeń w stosowaniu dyrektywy 95/46/WE – zarówno przez administratorów danych jak i podmioty danych, ale także niezależne organy nadzorcze, stało się podwalinami nowego prawa ochrony danych w Unii Europejskiej. Rozporządzenie opiera się na podstawowych wartościach tego istniejącego już systemu, utrzymując zasady ochrony danych oraz podstawy prawne przetwarzania danych, poddając je jedynie niezbędnym modyfikacjom.

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

W RODO podkreślono, że informowanie osób, których dane dotyczą, o wykorzystywaniu ich danych osobowych (prowadzeniu operacji przetwarzania) i celach, dla których jest ono prowadzone, jest niezbędne dla zapewnienia rzetelności i przejrzystości przetwarzania danych osobowych. Ogólne rozporządzenie o ochronie danych podkreśla jeszcze bardziej konieczność realizacji obowiązku informacyjnego. Od wszystkich administratorów danych wymagać się będzie, by wszelkie informacje kierowane do osób, których dane dotyczą, były formułowane jasnym i prostym językiem, by były zwięzłe i zrozumiałe. Szczególnie istotne będzie to zaś wówczas, gdy informacje i komunikaty będą kierowane do dzieci, które muszą móc je bez trudu zrozumieć. Ważną zmianą, jaką wprowadzi rozporządzenie, jest zwiększenie zakresu informacji, które należy przekazać. Od 25 maja 2018 r. administratorzy danych będą musieli poinformować również m.in. o okresie, przez który dane osobowe będą przetwarzane (retencja danych), o ewentualnym fakcie profilowania i jego konsekwencjach czy też o danych kontaktowych inspektora ochrony danych, jeśli został on wyznaczony.

Wszystkie dotychczasowe uprawnienia przysługujące osobom, których dane dotyczą zostały również zawarte w RODO. Novum będzie prawo do bycia zapomnianym, prawo do przenoszenia danych oraz prawo do tego, by nie podlegać profilowaniu.

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.

Uprawnienia GIODO na gruncie RODO.

Katalog uprawnień GIODO przyznanych przez RODO obejmuje w szczególności:

a) nakazywanie dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji jego zadań,

b) prowadzenie postępowań w formie audytów ochrony danych,

c) uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji jego zadań,

d) uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego,

e) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania,

f) nakazywanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia,

g) nakazywanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu,

h) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania,

i) zastosowanie, oprócz lub zamiast uprawnień określonych w art. 58 rozporządzenia, administracyjnej kary pieniężnej na mocy art. 83, zależnie od okoliczności konkretnej sprawy;

j) udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji

k) wydawanie, z własnej inicjatywy lub na wniosek, opinii przeznaczonych dla parlamentu narodowego, rządu państwa członkowskiego lub – zgodnie z prawem państwa członkowskiego – innych instytucji i organów oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną 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). Wobec stale zwiększającej się liczby spraw, którymi zajmuje się GIODO, rygor dwuinstancyjnego postępowania administracyjnego znacząco wpływa na efektywność i terminowość postępowania przez GIODO. Żeby usprawnić dochodzenie swoich praw przez obywateli, 27 stycznia 2017 r. GIODO przedstawił Ministrowi Cyfryzacji (resort ten jest odpowiedzialny za dostosowanie przepisów polskiego prawa do wymogów rozporządzenia) propozycję procedur postępowania przed organem nadzorczym przewidującą tryb odrębny prowadzenia tych postępowań, w tym jednoinstancyjność postępowania i możliwość przeprowadzania postępowania wyjaśniającego.

2. Rozpatrywanie skarg

W 2016 r. odnotowano znaczny wzrost w kilku kategoriach spraw, zwłaszcza dotyczących administracji publicznej, szeroko pojętej działalności marketingowej, służby zdrowia oraz w sprawach pracowniczych. Spadek nastąpił natomiast w liczbie skarg na przetwarzanie danych osobowych przez banki i inne instytucje finansowe.

Skargi w zakresie działalności marketingowej dotyczyły nieuwzględnienia sprzeciwu na przetwarzanie danych lub realizowania go ze znacznym opóźnieniem, lub wręcz dopiero po wszczęciu postępowania przed GIODO. Administratorzy zwykle tłumaczą powyższe błędem pracownika lub trudnościami technicznymi. Należy wskazać, że nowe rozporządzenie unijne wymaga, aby systemy, w których przetwarzane są dane osobowe, były tworzone w taki sposób, aby zapewniały prawidłową, skuteczną i niezwłoczną realizację nałożonych na nich obowiązków w tym zakresie. Wiele podmiotów ma również problem z dopełnianiem obowiązku informacyjnego realizowanego na wniosek lub spełnienia go tylko w części. Generalny Inspektor zauważa w tej materii błędy w interpretacji zakresu tego obowiązku zarówno przez wnioskujących, którzy wnosili o zbyt szeroki zakres, jak i przez zobowiązanych, którzy uchylali się od odpowiedzi na niektóre pytania. Należy zauważyć, że nowe rozporządzenie unijne zawiera daleko idące zwiększenie zakresu tego obowiązku, zatem konieczne jest przedsięwzięcie dalszych kroków w celu zwiększenia świadomości w tym zakresie, zarówno administratorów, jak i podmiotów danych.

Wzrost liczby skarg w sektorze służby zdrowia w roku 2016 związany był natomiast ze skargami na przetwarzanie danych osobowych w związku z realizacją obowiązkowych szczepień.

Jako temat skarg odżył także problem kopiowania dowodów osobistych. Generalny Inspektor wielokrotnie wskazywał, że administratorzy stosujący tego typu praktyki, pozyskują często - zwłaszcza w przypadku tzw. starych dowodów osobistych - zbyt szeroki zakres danych, wykraczający poza

ten, który jest im faktycznie potrzebny, a jednocześnie naruszają zasadę adekwatności. Z dowodami osobistymi wiąże się też, coraz rzadsza, ale jednak nadal występująca, praktyka zatrzymywania ich w zastaw za wypożyczany sprzęt. Dzieje się tak, mimo iż postępowanie to stanowi, zgodnie z ustawą o dowodach osobistych, wykroczenie, na co GIODO systematycznie zwraca uwagę.

Do Biura GIODO wpłynęło 2610 skarg dotyczących naruszenia przepisów o ochronie danych osobowych.

W 2016 r. do Biura GIODO wpłynęło 2610 skarg dotyczących naruszenia przepisów o ochronie danych osobowych. W porównaniu z rokiem 2015, w którym wpłynęło 2256 skarg, liczba ta uległa zwiększeniu o 354. Na skutek postępowań zainicjowanych skargami wydano 1205, decyzji administracyjnych, co stanowi niemal dwukrotny przyrost w porównaniu z latami poprzednimi (2015 r. - 646 decyzji, 2014 r. – 548 decyzji).

Każda ze skarg analizowana była na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego oraz wymogów fiskalnych wskazanych w ustawie o opłacie skarbowej . W sytuacji, gdy skarga nie spełniała warunków wymaganych przez ww. przepisy prawa, organ ochrony danych osobowych wzywał wnioskodawcę do uzupełnienia braków formalnych lub uiszczenia stosownej opłaty. Skutkiem powyższej analizy, w roku 2016 zostało zwróconych 389 skarg, z czego 151 z bieżącego okresu sprawozdawczego. Ponadto wiele ze skarg zostało pozostawionych bez rozpoznania w wyniku nieuzupełnienia braków formalnych.

Jeżeli w toku postępowania stwierdzono naruszenie przepisów ustawy o ochronie danych osobowych, Generalny Inspektor 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 roku sprawozdawczym GIODO w drodze decyzji administracyjnej **odmówił** uwzględnienia wniosku w 532 sprawach, 157 razy nakazywał przywrócenie stanu zgodnego z prawem, zaś w 319 przypadkach **umorzył** postępowanie. W postępowaniu odwoławczym wydano 188 decyzji, z których 130 utrzymało w mocy zaskarżone decyzje, zaś 58 **uchylało** w całości lub w części. Ponadto wydano 9 decyzji w postępowaniu o **stwierdzenie nieważności**, gdzie w 7 przypadkach stwierdzono nieważność, zaś w 2 **odmówiono** stwierdzenia nieważności.

W roku 2016 r. w postępowaniach zainicjowanych skargami oraz wszczętych przez Generalnego Inspektora Ochrony Danych Osobowych z urzędu, wydano **1205 decyzji, z których 60 zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie** (z czego 50 w czasie trwania

roku 2016). W porównaniu z rokiem 2015 nastąpił zatem nieznaczny wzrost liczby spraw trafiających do sądu, jednak należy mieć na uwadze, że w tym samym okresie wydano prawie dwa razy więcej decyzji.

Jednocześnie Wojewódzki Sąd Administracyjny w Warszawie w 24 sprawach dotyczących skarg na decyzje orzekł o oddaleniu skargi, zaś w 38 przypadkach uchylił zaskarżone decyzje (z czego 31 dotyczyło uchyleń w tzw. sprawach kościelnych). W 20 sprawach WSA orzekł o odrzuceniu skargi spowodowanym nieuzupełnieniem we wskazanym przez sąd terminie braków formalnych skarg, zaś w 8 przypadkach umorzył postępowanie.

Jeśli zaś chodzi o zakres tematyczny skarg, to można wyróżnić 15 podstawowych obszarów, takich jak: 1) administracja publiczna, 2) bezpieczeństwo publiczne, 3) sądy, prokuratury, komornicy, 4) banki i inne instytucje finansowe, 5) internet, 6) marketing, 7) mieszkalnictwo, 8) oświata i szkolnictwo wyższe, 9) służba zdrowia, 10) ubezpieczenia społeczne, majątkowe i osobowe, 11) telekomunikacja, 12) zatrudnienie, 13) windykacja, 14) związki wyznaniowe, 15) inne.

Kategoria spraw	Liczba skarg	Procentowo
Inne	559	21,4%
Administracja publiczna	327	12,5%
Internet	310	11,9%
Banki i inne instytucje finansowe	278	10,7%
Marketing	212	8,1%
Służba zdrowia	160	6,1%
Windykacja	131	5,0%
Telekomunikacja	128	4,9%
Zatrudnienie	128	4,9%
Mieszkalnictwo	79	3,0%
Ubezpieczenia społeczne, majątkowe i osobowe	75	2,9%
Sądy, prokuratury, komornicy	72	2,8%
Bezpieczeństwo publiczne	56	2,1%
Oświata i szkolnictwo wyższe	50	1,9%
Związki wyznaniowe	45	1,7%
SUMA	**2610**	**100%**

Tabela 1. ***Skargi rozpatrywane przez GIODO według kategorii tematycznych, w kolejności malejącej pod względem liczby.***

Porównanie liczby skarg na administratorów ze wskazanych wyżej sektorów w odniesieniu do roku 2014 i 2015 pozwala zauważyć następujące trendy. Po pierwsze, nastąpił dalszy **wzrost liczby skarg dotyczących szeroko pojętego przetwarzania danych osobowych przez administrację publiczną**, tj. wzrost o ponad 50 skarg w porównaniu z rokiem poprzednim (rok 2014 – 249, rok 2015 – 275, rok 2016 – 327). Skargi tego typu dotyczą głównie wymiany danych osobowych pomiędzy podmiotami oraz zamieszczania danych osobowych na stronach internetowych jednostek samorządu terytorialnego w związku z udostępnianiem informacji publicznej. Drugi zauważalny **wzrost nastąpił w sprawach dotyczących służby zdrowia**, gdzie liczba skarg w porównaniu z rokiem poprzednim wzrosła o 101 (rok 2014 - 47, rok 2015 – 59, rok 2016 – 160). Głównym tego powodem był liczny napływ skarg na przetwarzanie danych osobowych w związku ustawowym obowiązkiem szczepień. **Dużym skokiem w liczbie złożonych skarg charakteryzowały się sprawy dotyczące marketingu** (rok 2014 – 153, rok 2015 – 95, rok 2016 – 212) oraz **dotyczące przetwarzania danych osobowych w związku z zatrudnieniem** (rok 2014 – 62, rok 2015 – 47, rok 2016 – 128). Duży spadek liczby skarg, bo aż o 51, odnotować zaś można w odniesieniu do działalności bankowej i instytucji finansowych (rok 2014 – 354, rok 2015 – 329, rok 2016 – 278). Nieznaczny wzrost nastąpił w kategoriach dotyczących ubezpieczeń społecznych, majątkowych i osobowych (rok 2014 – 63, rok 2015 – 55, rok 2016 – 75) oraz windykacji (rok 2014 – 110, rok 2015 – 110, rok 2016 – 131). W pozostałych kategoriach spraw, w porównaniu z rokiem poprzednim, liczba skarg utrzymała się na podobnym poziomie a jeśli spadła lub wzrosła, to nieznacznie. Dotyczy to zwłaszcza skarg związanych z oświatą i szkolnictwem wyższym (rok 2014 – 51, rok 2015 – 47, rok 2016 – 50), spraw dotyczących mieszkalnictwa (rok 2014 – 104, rok 2015 – 81, rok 2016 – 79) oraz telekomunikacji (rok 2014 – 134, rok 2015 – 135, rok 2016 – 128).

2.1. Administracja publiczna

W 2016 r. wpłynęło 327 skarg na podmioty z sektora administracji publicznej, co stanowi 12,5% ogółu skarg (2014 r. – 249, 2015 r. – 275).

Dotychczas najczęstszym przypadkiem skarg na przetwarzanie danych osobowych przez podmioty należące do administracji publicznej były skargi na publikacje danych osobowych na stronach internetowych w związku z realizowaniem obowiązku udzielenia informacji publicznej. Obecnie jednak głównym przedmiotem skarg ponownie stają się sprawy fundamentalne, jak podstawa przetwarzania danych osobowych czy zakres żądanych informacji.

Jak co roku, przeważająca liczba skarg dotyczyła braku zanonimizowania danych osobowych przed ich opublikowaniem w Biuletynie Informacji Publicznej. Skarżący często wskazywali również na podejrzenie braku podstaw do przetwarzania danych, co jednak zazwyczaj nie znajdowało potwierdzenia w toku postępowania.

Generalny Inspektor ponownie zwrócił uwagę na problem zamieszczania informacji publicznych w Biuletynach Informacji Publicznej bez dokonania anonimizacji tych dokumentów poprzez usunięcie z nich danych osób fizycznych składających skargi. Nie negując konieczności udostępnienia ww. informacji, GIODO wskazuje, że administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest zobowiązany zapewnić, aby te dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Udostępniając informację publiczną, administrator danych obowiązany jest ustalić, czy zakres przekazywanych danych jest niezbędny dla potrzeb takiego udostępnienia. W ocenie Generalnego Inspektora Ochrony Danych Osobowych upublicznianiu uchwały jedynie w celu informacyjnym, zbędne jest ujawnianie imion i nazwisk osób, których ona dotyczy.

Z kolei nie każde udostępnienie danych osobowych na stronie internetowej będzie świadczyło o naruszeniu przepisów ustawy o ochronie danych osobowych. W jednej ze spraw skarżąca podniosła, że na stronie internetowej Biuletynu Informacji Publicznej upubliczniono jej dane osobowe bez jej zgody. W czasie postępowania ustalono, że udostępnienie danych nastąpiło w związku z interpelacją radnego w zakresie zleceń zawartych przez placówki szkolne na przeprowadzenie szkoleń. Dane osobowe skarżącej zostały opublikowane nie jako osoby fizycznej, ale w związku prowadzoną przez nią działalnością gospodarczą w tym zakresie. Generalny Inspektor wskazał, że przepisy o ochronie danych osobowych nie znajdują zastosowania w niniejszej sprawie, tj. gdyż nie chronią danych osobowych przedsiębiorców ani adresu prowadzonej przez nich działalności gospodarczej [3].

W jednej ze spraw Generalny Inspektor zwrócił uwagę na konieczność dostosowania procesu rekrutacyjnego do przepisów ustawy o ochronie danych osobowych i innych ustaw[4]. Wójt jednej z gmin, w związku z prowadzoną rekrutacją, żądał od osób ubiegających się o zatrudnienie danych dotyczących ich stanu zdrowia oraz kopii dowodu osobistego, dla potwierdzenia posiadania obywatelstwa polskiego. W art. 22^1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy[5] ustawodawca precyzyjnie określa, jakich danych osobowych ma prawo żądać pracodawca od osoby ubiegającej się o zatrudnienie. Zakres wymaganych dokumentów został natomiast sprecyzowany w rozporządzeniu wydanym na podstawie delegacji ustawowej zawartej w art. 298^1 ww. ustawy[6]. Zgodnie z powyższym, pracodawca może żądać m.in. dokumentów potwierdzających kwalifikacje zawodowe, wymagane do wykonywania oferowanej pracy, orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na określonym stanowisku oraz innych dokumentów, jeżeli obowiązek ich przedłożenia wynika z odrębnych przepisów. Należy przy tym podkreślić, że orzeczenia lekarskiego o przeciwwskazaniach nie należy utożsamiać z zaświadczeniem o stanie zdrowia. Zakres przetwarzanych danych został zatem ściśle określony przez ustawodawcę. Przetwarzanie danych osobowych wykraczających poza ten zakres wymaga dobrowolnie wyrażonej zgody, jednak

[3] Decyzja GIODO z dnia 23 sierpnia 2016 r. (DOLiS/DEC-751/16).
[4] Pismo GIODO z 15 marca 2016 r. (DOLiS-440-7/16/I/18049/16).
[5] t.j. Dz. U. z 2016 r., poz. 1666 ze zm.
[6] 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. z 1996 r. Nr 62, poz. 286 ze zm.).

zgodnie z ugruntowanym w tej materii orzecznictwem, brak równowagi w relacjach pracownik-pracodawca podaje w wątpliwość dobrowolność takiej zgody[7].

W innej ze spraw Generalny Inspektor wezwał organ podatkowy do zapewnienia zgodności przetwarzania danych osobowych z zasadami legalności, celowości i proporcjonalności[8]. Do akt postępowania podatkowego załączono dane osobowe pełnomocnika strony z aplikacji podatkowej POLTAX. Jako powód takiego postępowania organ podatkowy wskazał konieczność ustalenia adresu korespondencyjnego pełnomocnika. Zdaniem GIODO, zgodnie z zasadami wyrażonymi w art. 26 ustawy, 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. Skuteczne doręczanie korespondencji nie wymaga przetwarzania informacji wykraczających poza niezbędne w tym celu minimum (np. dane zostały wskazane przez pełnomocnika). W sprawie tej, która stała się przyczynkiem do skierowania przez GIODO stosownego wystąpienia, naczelnik organu podatkowego wyłączył z akt postępowania wytworzony wydruk, w związku z czym Generalny Inspektor umorzył prowadzone postępowanie administracyjne[9].

2.2. Bezpieczeństwo publiczne

W 2016 roku do GIODO wpłynęło 56 skarg dotyczących szeroko pojętego bezpieczeństwa państwa i porządku publicznego.

W porównaniu z rokiem poprzednim nastąpił ich niewielki wzrost (rok 2014 – 78, rok 2015 – 43). Spośród nich zdecydowana większość dotyczyła przetwarzania danych osobowych w Systemie Informacyjnym Schengen lub Krajowym Systemie Informacyjnym Policji.

Przykładowo, Generalny Inspektor utrzymał w mocy decyzję odmawiającą uwzględnienia wniosku skarżącego o usunięcie jego danych osobowych z Krajowego Systemu Informacyjnego Policji[10]. W treści skargi podniesiono, że nie zachodzą okoliczności, które uzasadniałyby dalsze przechowywanie w rejestrze danych osobowych skarżącego, zważywszy na charakter popełnionego czynu, jak i samo zachowanie skarżącego, a przede wszystkim zatarcie skazania zarządzone postanowieniem sądu rejonowego. W decyzji ponownie wskazano, że prawo do ochrony danych osobowych nie jest prawem absolutnym i może ulec ograniczeniu z uwagi na interes państwa, polegający na zapewnieniu ładu i porządku publicznego oraz bezpieczeństwa jego obywateli. W toku postępowania ustalono, że podstawą prawną przetwarzania danych osobowych osób, wobec których były prowadzone postępowania przez Policję, stanowi art. 20 ust. 1 ustawy o Policji[11], z ograniczeniami wynikającymi z art. 19 tej ustawy. Jak wskazano, KSIP nie stanowi rejestru osób skazanych czy

[7] Tak w wyroku NSA z dnia 1 grudnia 2009 r., sygn. akt I OSK 249/09.
[8] Pismo GIODO z 23 czerwca 2016 r. (DOLiS-440-947/14/56592/16).
[9] Decyzja GIODO z 23 czerwca 2016 r. (DOLiS/DEC-529/16).
[10] Decyzja GIODO z 27 stycznia 2016 r. (DOLiS/DEC-78/16).
[11] Ustawa z dnia 6 kwietnia 1990 r. o policji (t.j. Dz. U. z 2016 r., poz. 1782 ze zm.).

też ukaranych, gdyż taką funkcję pełni Krajowy Rejestr Karny. KSIP jest policyjnym zbiorem danych gromadzącym informacje o wszczętych i prowadzonych przez Policję postępowaniach. Informacje zawarte w KSIP nie stanowią źródła wiedzy powszechnie dostępnej, i służą do realizacji wyłącznie zadań Policji. Sąd administracyjny odrzucił skargę skarżącego na decyzję wydaną w omawianej sprawie, podzielając ocenę prawną dokonaną przez Generalnego Inspektora[12]. Jak wskazał Sąd, z przepisów jednoznacznie wynika, że organy Policji są uprawnione do przetwarzania danych osób również po zakończeniu prowadzonych przez nie postępowań, nie wyłączając danych osób, w stosunku do których skazanie uległo zatarciu. To również organy Policji dokonują oceny przydatności zebranych informacji. Tym samym sądy administracyjne kontynuują dotychczasową linię orzeczniczą[13].

W zakresie Systemu Informacji Schengen, pisma dotyczyły zazwyczaj zapytań obcokrajowców odnośnie do umieszczenia ich danych osobowych w tym systemie.

2.3. Sądy, prokuratury, komornicy

W roku 2016 do GIODO wpłynęły 72 skargi dotyczące działalności sądów, prokuratur i komorników.

Tym samym zanotowano niewielki wzrost względem poprzedniego okresu sprawozdawczego, w którym wpłynęło w tej kategorii 58 skarg. (rok 2014 – 67, rok 2015 – 58, rok 2016 – 72). Sprawy tego rodzaju dotyczą najczęściej zarzutu udostępnienia danych osobowych osobom do tego nieuprawnionym.

Przedmiotem jednej ze skarg było opublikowanie imienia i nazwiska skarżącej w wyroku Trybunału Konstytucyjnego na stronie internetowej. W sentencji tego wyroku znajdowały się dane szczególnie chronione dotyczące stanu zdrowia, przebytych chorób czy podjętego leczenia. Generalny Inspektor dokonał rozgraniczenia pomiędzy publikacją pełnej treści wyroku w Dzienniku Ustaw a publikacją w Biuletynie Informacji Publicznej. W drodze decyzji administracyjnej nakazał usunięcie zaistniałych nieprawidłowości poprzez usunięcie z wyroku zamieszczonego na stronie internetowej, która pełni rolę Biuletynu Informacji Publicznej, danych osobowych skarżącej, tj. jej imienia i nazwiska. Stanowisko GIODO podzielił WSA w Warszawie, oddalając skargę Prezesa Trybunału Konstytucyjnego na decyzję GIODO[14].

[12] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 12 października 2016 r. (sygn. akt II SA/Wa 540/16).
[13] Wyrok WSA z dnia 28 stycznia 2014 r. (sygn. akt II SA/Wa 1366/13), wyrok NSA z dnia 22 marca 2013 r. (sygn. akt I OSK 786/12), wyrok NSA z dnia 19 grudnia 2011 r. (sygn. akt I OSK 1100/11), wyrok NSA z dnia 17 lipca 2015 r. (sygn. akt I OSK 182/14).
[14] Wyrok WSA w Warszawie z dnia 19 stycznia 2017 r. (sygn. akt II SA/Wa 1434/16), wyrok jest prawomocny.

2.4. Banki i inne instytucje finansowe

W 2016 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło 278 skarg na podmioty z sektora finansowego.

W skargach kwestionowano legalność przetwarzania danych osobowych przez banki i inne instytucje finansowe, co stanowiło 10,7% ogółu skarg (dla porównania w roku 2015 – 329, w 2014 – 354). Tym samym jest to jedna z najliczniejszych kategorii skarg jakie wpływają do urzędu.

Przedmiot wnoszonych skarg pozostaje niezmienny od kilku lat. Wątpliwości dotyczą głównie podstaw prawnych przetwarzania, zakresu pozyskiwanych danych, a przede wszystkim udostępniania danych osobowych Biuru Informacji Kredytowej, tj. podmiotowi utworzonemu na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[15] w celu gromadzenia, przetwarzania i udostępniania informacji stanowiących tajemnicę bankową na rzecz banków i innych instytucji finansowych w zakresie, w jakim informacje te są potrzebne m.in. w związku z wykonywaniem czynności bankowych.

Istotnym problemem w zakresie przetwarzania danych osobowych przez szeroko pojęte instytucje finansowe stało się nieodnotowywanie sprzeciwu na przetwarzanie danych osobowych w celach marketingowych, odnotowywanie go z opóźnieniem czy wręcz dopiero po wniesieniu skargi i interwencji GIODO. Należy zauważyć, że za odnotowanie skutecznego sprzeciwu odpowiada administrator danych osobowych, nawet w sytuacji, jeżeli z wewnętrznych ustaleń administratora wynika, że uchybienie wyniknęło z niezastosowania się pracownika do wewnętrznych procedur. Ten sam problem dotyczy opóźnień w spełnianiu obowiązku informacyjnego realizowanego na wniosek podmiotu danych (art. 33 w zw. z art. 32 ust. 1 ustawy). Zgodnie z prawem, administrator danych osobowych powinien udzielić wnioskowanych informacji w terminie 30 dni. Termin ten nierzadko jest przekraczany przez administratorów. Wprawdzie przygotowanie odpowiedzi przez podmioty posiadające duże zasoby informacji wymaga czasu, to jednak należy wskazać, że ustawa nie wprowadza żadnych wyjątków w tym zakresie i nie przewiduje wydłużenia określonego w ustawie terminu. Instytucje finansowe powinny zatem, jak każdy administrator danych, rzetelnie i terminowo spełniać ww. obowiązek. Prawidłowe poinformowanie osoby, której dane dotyczą, o przysługujących jej prawach oraz przekazanie jej informacji o procesie przetwarzania jej danych (w zakresie określonym w art. 32 ust. 1 pkt. 1-5a ustawy) stanowi podstawową gwarancję prawa do kontroli przetwarzania jej danych osobowych. Niedopełnienie ww. obowiązku uniemożliwiające korzystanie z praw może podlegać odpowiedzialności karnej na podstawie art. 54 ustawy.

Stałym powodem skarg jest również udostępnianie danych osobowych na rzecz instytucji,

[15] t.j. Dz. U. z 2016 r., poz. 1988 ze zm.

o których mowa w art. 105 ust. 4 Prawa bankowego, których zadaniem jest gromadzenie przetwarzanie i udostępnianie informacji stanowiących tajemnicę bankową na rzecz instytucji finansowych (np. w celu oceny zdolności kredytowej klienta).

Dużo wątpliwości budzi też praktyczna realizacja art. 105a ust. 3 Prawa bankowego, w myśl którego banki i inne wskazane w tym przepisie instytucje, mogą przetwarzać informacje stanowiące tajemnicę bankową i inne udostępnione informacje dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub innymi instytucjami, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z zawartej umowy tego rodzaju, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez tę instytucję, o zamiarze przetwarzania dotyczących jej informacji, bez jej zgody. Dane te, zgodnie z art. 105a ust. 1 Prawa bankowego, mogą być przetwarzane w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Brak spełnienia ww. przesłanek stanowi przeszkodę w przetwarzaniu przez te podmioty tak zebranych danych.

Problemem jest brak wskazania w Prawie bankowym formy spełnienia ww. obowiązku informacyjnego. Wprawdzie przepisy Prawa bankowego nie formułują obowiązku spełnienia ww. obowiązku informacyjnego w formie listu poleconego ze zwrotnym potwierdzeniem odbioru, to zgodnie z zasadą wyrażoną w art. 26 ustawy o ochronie danych osobowych, na administratorze danych, ciąży obowiązek dochowania szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Kwestia skutecznego poinformowania o spełnieniu przesłanek warunkujących przetwarzanie informacji bez zgody osoby, której dane dotyczą, po wygaśnięciu zobowiązania, ciąży na podmiocie, który chce dokonać takiego wpisu. Instytucje finansowe powinny zatem podjąć takie starania i takie środki, które będą gwarantowały prawidłowe i skuteczne poinformowanie o zamiarze dalszego przetwarzania danych[16].

Na bankach ciąży też obowiązek aktualizacji danych osobowych. Ustawa nakłada na administratorów obowiązek dołożenia szczególnej staranności w przetwarzaniu danych osobowych, zwłaszcza obowiązek zapewnienia, aby dane te były merytorycznie poprawne (art. 26 ust. 1 pkt 3). Oznacza to, że informacje przetwarzane przez administratora powinny być zgodne z prawdą, kompletne i odpowiadające aktualnemu stanowi rzeczy. Każda aktualizacja powinna zatem nastąpić bez zbędnej zwłoki (tj. w czasie nie dłuższym niż konieczny z obiektywnych przyczyn) – jako wyraz szczególnej staranności banków. W jednej ze spraw skarżąca zakwestionowała niezaktualizowanie jej danych osobowych przez bank w instytucji, o której mowa w art. 105 ust. 4 Prawa bankowego, pomimo dokonania spłaty kredytu wraz z należnymi odsetkami[17]. W sporządzonym raporcie, pomimo znacznego upływu od spłaty, zobowiązanie nadal widniało ze statusem „w windykacji". Pomimo interwencji zainteresowanej, stan ten nie został zmieniony. Dopiero po kilku miesiącach bank zaktualizował dane skarżącej w zakresie zobowiązania. Bank poinformował jednocześnie, że podejmie

[16] Decyzja GIODO z 13 stycznia 2016 r. (DOLiS/DEC-12/16) oraz wyrok WSA w Warszawie z dnia 28 lipca 2016 r. o sygn. akt II SA/Wa 461/16, decyzja GIODO z 25 listopada 2016 r. (DOLiS/DEC-1230/16); patrz również wyrok WSA w Warszawie z dnia 5 sierpnia 2016 r. o sygn. akt II SA/Wa 2147/15, Wyrok WSA w Warszawie z dnia 12 maja 2016 r. o sygn. akt II SA/Wa 1713/15 (nieprawomocny), wyrok WSA w Warszawie z dnia 18 sierpnia 2015 r. o sygn. akt II SA/Wa 11/15 (nieprawomocny).

[17] Decyzja GIODO z 29 czerwca 2016 r. (DOLiS/DEC-547/16).

działania w celu wyeliminowania zauważonych nieprawidłowości.

Powracającym rokrocznie problemem jest przetwarzanie danych osobowych dla celów marketingowych po zalogowaniu do internetowego serwisu transakcyjnego, pomimo wyrażonego sprzeciwu.

Przytoczone w sprawozdaniu za rok 2015 r. podjęte przez Generalnego Inspektora rozstrzygnięcie w sprawie przetwarzania danych osobowych dla celów marketingowych polegających na kierowaniu informacji handlowych w internetowym serwisie transakcyjnym po zalogowaniu do niego klienta, pomimo zgłoszonego sprzeciwu na przetwarzanie w tym celu, zyskało akceptację sądu administracyjnego. W sprawie tej Generalny Inspektor nakazał bankowi przywrócenie stanu zgodnego z prawem w procesie przetwarzania danych osobowych skarżącego poprzez zaprzestanie przetwarzania jego danych osobowych w celu marketingu produktów[18]. W związku ze złożoną przez spółkę skargą, w toku postępowania sądowo-administracyjnego sąd zgodził się jednak z organem, że upowszechnianie informacji o towarach i usługach, podejmowanie działań w celu zainteresowania klienta nowymi produktami i zachęcenie go do zakupu, stanowi reklamę. Informację o nowych produktach stanowi działanie marketingowe, ze względu na podkreślenie atrakcyjności oferty i nakłanianie do skorzystania z niej. W ocenie sądu, informowanie klienta na jego indywidualnym profilu o produktach banku (prezentowana po zalogowaniu na osobnej zakładce) stanowi niewątpliwie przetwarzanie jego danych osobowych w celach marketingowych[19]. Jednocześnie sąd podkreślił, że decyzja Generalnego Inspektora nie zabrania bankowi prowadzenia działalności marketingowej i umieszczania na stronie reklam produktów, a jak określono „[o]organ zabrania jedynie takiej formy działań marketingowych, gdy obywatel ten korzysta z prawa przyznanego przepisem art. 32 ust. 1 pkt 8 ustawy o ochronie danych osobowych”[20].

Należy wziąć pod uwagę, że zgodnie z zasadą *privacy by design* wyrażoną w art. 25 ogólnego rozporządzenia o ochronie danych osobowych, administrator winien już na etapie projektowania wdrażać odpowiednie środki techniczne i organizacyjne w celu skutecznej realizacji zasad ochrony danych oraz praw osób, których dane dotyczą. Powyższa zasada dotyczy również prawidłowego odnotowania i zastosowania w swoich systemach sprzeciwu podmiotu danych na przetwarzanie w celach reklamowania swoich usług lub produktów. a zwłaszcza odnotowanie powinno być skuteczne. Instytucje finansowe i inne, powinny wziąć pod uwagę przyszłe uregulowania w tym zakresie.

Z doświadczenia organu wynika, że podmioty powinny zwrócić uwagę na prawidłowe spełnienie obowiązku informacyjnego realizowanego na wniosek zgodnie z art. 33 ustawy. Obowiązek udzielenia informacji wskazanych w art. 32 ust. 1 pkt 5 ustawy dotyczy informacji o sposobie udostępnienia danych., w szczególności informacji o odbiorcach, lub kategoriach odbiorców, którym te dane są udostępniane. Zakres nie został zatem *stricte* zawężony do definicji legalnej odbiorcy wskazanej w art. 7 pkt 6 ustawy. Stanowi zatem katalog otwarty.

Generalny Inspektor zauważa jednak, że określenie zakresu obowiązku informacyjnego sta-

[18] Decyzja GIODO z dnia 16 grudnia 2015 r. (DOLiS/DEC-960/15).
[19] Wyrok WSA w Warszawie z dnia 12 sierpnia 2016 r., sygn. akt II SA/Wa 337/16 (nieprawomocny).
[20] Podobnie wyrok WSA w Warszawie z dnia 9 października 2015 r., sygn. akt II SA/Wa 40/15 (nieprawomocny).

nowi problem również dla samych uprawnionych. W innej sprawie Generalny Inspektor również nakazał spełnienie obowiązku informacyjnego w ww. zakresie, a konkretnie wskazanie podmiotów przetwarzających dane w związku z zawartą umową powierzenia[21]. Jednocześnie Generalny Inspektor odmówił uwzględnienia wniosku w zakresie udzielenia informacji o podmiocie będącym właścicielem serwerów oraz ich lokalizacji oraz sposobie zabezpieczenia danych przed dostępem osób trzecich. W powyższym zakresie bank nie udzielił odpowiedzi skarżącemu. Bank ma prawo do udostępnienia takich informacji, ale nie obowiązek. Udzielenie takich informacji należy do decyzji banku, gdyż są to informacje wrażliwe dla instytucji ze względu na jej bezpieczeństwo[22]. Generalny Inspektor uznał, że takie informacje wykraczają poza zakres obowiązku informacyjnego realizowanego na wniosek. Podobnie w zakres obowiązku informacyjnego nie będą wchodzić dane osobowe konkretnych pracowników, które przetwarzały dane osobowe, w tym wydane upoważnienia dla tych osób[23].

Jednocześnie obowiązku informacyjnego z art. 33 ustawy o ochronie danych osobowych nie należy mylić z innymi uprawnieniami informacyjnymi, regulowanymi przez ustawy odrębne, których zastosowanie znajduje pierwszeństwo przed ustawą o ochronie danych osobowych, np. wniosku o wydanie informacji, o których mowa w art. 23 ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (t.j. Dz. U. z 2014 r., poz. 1015 ze zm.)[24].

W przypadku stosowania środków komunikacji elektronicznej w kontaktach z klientem należy zwrócić szczególną uwagę na poprawność danych kontaktowych. Problem dotyczy głównie adresów e-mail, których nazwy mogą być czasem mylące lub łudząco podobne do innych. W szczególności może dojść do pomyłek w przypadku odręcznego zapisywania adresów e-mail . Błąd w adresie może natomiast spowodować nieuprawnione udostępnienie danych osobowych. Jedna z takich sytuacji stała się przedmiotem skargi do GIODO, jednak ze względu na zaktualizowanie adresu pocztowego umorzono postępowanie[25]. Należy przy tym zauważyć, że błędny adres pocztowy może wynikać z błędnego jego podania przez klienta. Podmioty, które korzystają z tej formy komunikacji, powinny przedsięwziąć kroki, które dodatkowo potwierdzą prawidłowość adresu przed przesłaniem właściwej korespondencji wynikającej z umowy. Zgodnie z art. 26 ust. 1 pkt 3 ustawy, administrator powinien zapewnić, aby dane były merytorycznie poprawne.

[21] Decyzja GIODO z 22 grudnia 2016 r. (DOLiS/DEC-1397/16).
[22] Nie wolno ujawniać dokumentacji związanej z zabezpieczaniem informacji i danych osobowych, http://www.giodo.gov.pl/222/id_art/9906/j/pl/
[23] Decyzja GIODO z 11 października 2016 r. (DOLiS/DEC-994/16).
[24] Decyzja GIODO z 18 lutego 2016 r. (DOLiS/DEC-147/16/).
[25] Decyzja GIODO z 8 kwietnia 2016 r. (DOLiS/DEC-255/16).

2.5. Internet

W 2016 r. skargi dotyczące przetwarzania danych osobowych skarżących w sieci Internet stanowiły znaczącą liczbę – wpłynęło 310 skarg, co stanowiło 11,9% ogółu.

Częstym tematem skarg kierowanych do GIODO jest odmowa udostępnienia danych osobowych użytkowników portalu internetowego[26]. W jednej ze spraw skarżący poinformowali administratora w trybie art. 14 ust. 1 ustawy o świadczeniu usług drogą elektroniczną[27], że w prowadzonym przez niego serwisie internetowym zamieszczone są wpisy, które naruszają ich dobra osobiste. Skarżący wezwali zatem do usunięcia niezgodnych z prawem wpisów oraz podania numerów IP użytkowników, którzy je zamieścili. Skarżący uzasadnili swój wniosek zamiarem dochodzenia ochrony swoich dóbr osobistych na drodze postępowania cywilnego. W ocenie GIODO, wniosek znajdował uzasadnienie prawne w art. 23 ust. 1 pkt 5 ustawy i jako taki powinien zostać przez administratora uwzględniony. Odmowa udostępnienia IP komputerów autorów wpisów w żądanym przez skarżących zakresie uniemożliwiałaby podjęcie jakichkolwiek dalszych działań służących takiej identyfikacji tych osób, która pozwoli na skuteczne zainicjowanie przeciwko nim planowanych działań przed sądem. W sytuacji, gdy osoba, która chce podjąć dalsze kroki na drodze sądowej, nie dysponuje zasadniczo żadnymi informacjami o autorach wpisów – poza tymi, które związane są z opublikowaną wiadomością (adresem IP, datą, nazwą użytkownika) – zasadne jest przyjęcie, że podejmowane przez nich działanie służące ustaleniu tożsamości tych osób, mieści się w pojęciu ich prawnie usprawiedliwionego celu. Adres IP może natomiast stanowić daną osobową, gdyż w określonych okolicznościach jest informacją umożliwiającą identyfikację konkretnej osoby fizycznej[28].

W innej sprawie skarżący zwrócił się do GIODO o nakazanie spółce cywilnej prowadzącej stronę internetową udostępnienia na jego rzecz danych osobowych w zakresie imienia i nazwiska, a także adresu oraz numeru IP komputera podmiotu, który udostępnił ogłoszenie o pracę. W opisywanej sprawie skarżący był przekonany, że wskazane ogłoszenie było fałszywe i doszło do wyłudzenia jego danych osobowych. Spółka odmówiła żądaniu skarżącego. Generalny Inspektor nakazał spółce udostępnienie adresu IP, gdyż tylko takie dane posiadała[29]. Analiza materiału dowodowego wskazywała, że żądanie skarżącego było w pełni uzasadnione i wypełniało dyspozycję art. 23 ust. 1 pkt 5 ustawy. Skarżący wiarygodnie uzasadnił potrzebę pozyskania danych zamiarem wszczęcia postępowania sądowego mającego na celu ochronę jego dóbr osobistych.

[26] Decyzja GIODO z 30 listopada 2016 r. (DOLiS/DEC-1263/16).
[27] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. Z 2016 r. poz. 1030 ze zm.).
[28] Patrz wyrok NSA z dnia 19 maja 2011 r., sygn. akt I OSK 1079/10.
[29] Decyzja GIODO z 27 maja 2016 r. (DOLiS/DEC-420/16).

2.6. Marketing

W 2016 roku do Biura GIODO wpłynęło 212 skarg dotyczących marketingu.

Skargi na podmioty z tego sektora dotyczą głównie szeroko pojętej działalności mającej zachęcić do kupna produktów lub usług. W zdecydowanej większości skargi dotyczą podejmowania działań marketingowych mimo złożonego przez te osoby sprzeciwu, tj. skorzystania z uprawnienia przewidzianego w art. 32 ust. 1 pkt 8 ustawy.

Podobnie jak w sektorze bankowym, częstym problemem jest niedopełnienie obowiązku rejestracji sprzeciwu na przetwarzanie danych osobowych w celach marketingowych zgodnie z ustawą, co stanowi naruszenie zasad legalnego przetwarzania danych osobowych[30]. Administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczelności jest obowiązany zapewnić, aby ich dane były przetwarzane zgodnie z prawem oraz zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (art. 26 ust. 1 pkt. 1 i 2 ustawy). Administrator danych osobowych jest zobowiązany do zastosowania takich rozwiązań technicznych i organizacyjnych, które zagwarantują prawidłowe przetwarzanie danych, w tym skuteczne i natychmiastowe uwzględnianie sprzeciwów osób, których dane osobowe są przetwarzane w celach marketingowych.

Tymczasem administratorzy zwykle tłumaczą powyższe błędem pracownika lub trudnościami technicznymi.

Należy wskazać, że nowe rozporządzenie unijne[31] wymaga, aby systemy, w których przetwarzane są dane osobowe, były tworzone w taki sposób, by zapewniały prawidłową, skuteczną i niezwłoczną realizację obowiązków w tym zakresie nałożonych na administratorów danych.

Ze względu na to, że sytuacje, w której pomimo niewyrażenia zgody na przetwarzanie danych osobowych w celach marketingowych albo złożeniu sprzeciwu na takie przetwarzanie, w dalszym ciągu do osób tych kierowany jest marketing usług własnych administratora są bardzo częste, sprawy te stały się dla GIODO impulsem do kierowania wystąpień do administratorów danych w tym zakresie. Przede wszystkim zwracano się o wprowadzenie rozwiązań organizacyjnych, które wyeliminują takie zdarzenia w przyszłości. Ponadto wskazywano, że spółka, jako administrator, powinna niezwłocznie realizować prawa osób, których dane dotyczą, a zatem w sposób niepowodujący konieczności wielokrotnego występowania przez podmioty danych ze sprze-

[30] Decyzja GIODO z dnia 30 sierpnia 2016 r. (DOLiS/DEC-776/16).

[31] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – Dz.Urz.UE L 119 z dnia 4 maja 2016 r.

ciwem na przetwarzanie ich danych osobowych w celach marketingowych[32]. Wskazywano także na niedopuszczalność takich sytuacji i konieczność wprowadzenia przez administratora rozwiązań technicznych i organizacyjnych zapobiegających ich powstawaniu w przyszłości[33].

O ile natychmiastowe zastosowanie sprzeciwu może być utrudnione w przypadku przesyłek listowych, o tyle w przypadku stosowania mailingu[34], nie powinno to nastręczać większych problemów. Konieczność zapobieżenia błędom migracji systemu mailingowego, w wyniku którego omyłkowo zaimportowano dane, co do których wyrażono sprzeciw na przetwarzanie w celach marketingowych, ciąży na administratorze danych, który powinien przedsięwziąć działania w celu niedopuszczenia do zaistnienia takich sytuacji[35].

Generalny Inspektor wskazuje również, że administrator danych, jest uprawniony do przetwarzania danych osobowych w celu prowadzeniu marketingu własnych produktów lub usług w przypadku, gdy łączy go z aktualnym klientem umowa (art. 23 ust. 1 pkt 5) albo gdy osoba ta wyraziła na to zgodę (art. 23 ust. 1 pkt 1 ustawy). Administrator jest zobowiązany do przetwarzania danych swoich dotychczasowych (czyli byłych) klientów wyłącznie dla realizacji celów archiwalnych lub rachunkowych. Przetwarzanie danych osobowych klientów do celów marketingowych, w przypadku zakończenia umowy, tylko za ich odrębną zgodą. Administrator nie jest zatem uprawniony do przetwarzania danych osobowych byłego klienta w celach marketingowych, jeżeli nie łączy go z nim już żadna umowa, lub nie wyraził on zgody na tego rodzaju przetwarzanie po jej zakończeniu.

2.7. Mieszkalnictwo

W 2016 roku skargi dotyczące zagadnień związanych z mieszkalnictwem stanowiły 3% ogółu. Do Biura GIODO wpłynęło ich bowiem 81 () (dla porównania w roku 2014 r. – 104, w 2015 – 81).

Częstym, podnoszonym od kilku lat problemem jest informowanie o zadłużeniach na klatkach schodowych. Generalny Inspektor wielokrotnie wskazywał, że na administratorze danych ciąży obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, co znajduje swoją materializację m.in. w obowiązku zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii przetwarzanych danych. Przede wszyskim powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym (art. 36 ustawy). Tymczasem upublicznienie danych na klatkach schodowych prowadzi właśnie do udostępnienia danych osobowych osobom nieupoważnionym (innym niż człon-

[32] Pismo z 30 sierpnia 2016 r. (DOLIS-440-2246/15/77203/16).
[33] Pismo z 1 grudnia 2016 r. (DOLiS-440-102/14/104015/16).
[34] Niezależnie od wymagań określonych w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne .
[35] Decyzja GIODO z 12 grudnia 2016 r. (DOLiS/DEC-1411/16).

kowie wspólnoty, np. lokatorom wynajmującym mieszkanie, osobom odwiedzającym). Nieuiszczanie należnych opłat jest niewątpliwie problemem całej wspólnoty iwywieszanie ogłoszeń o stanie zadłużenia poszczególnych lokali jest jedną z form społecznego nacisku na jednostki, które tych opłat nie wnoszą, jednak administratorzy powinni w tym zakresie zachować szczególną staranność. Zdaniem Generalnego Inspektora, praktykę udostępniania w miejscu publicznie dostępnym informacji zawierających dane osobowe należy uznać za nieprawidłową. Takie postępowanie może narażać spółdzielnię lub wspólnotę na zarzut udostępnienia danych osobowych bez podstawy prawnej, w tym na zarzut niedopełnienia szczególnej staranności w ochronie danych osobowych lub niewłaściwego ich zabezpieczenia[36].

Z kolei w innej ze spraw skarżąca zarzuciła udostępnienie jej danych osobowych przez wspólnotę mieszkaniową na rzecz właścicieli nieruchomości. Skarżąca zakwestionowała zwłaszcza legalność stworzenia przez zarząd wspólnoty broszury zawierającej jej dane osobowe i historię jej postępowań sądowych wobec wspólnoty, a także udostępnienie tej publikacji wśród wspólnoty. Jak wyjaśniała wspólnota, broszura dokumentowała działanie zarządu i była odpowiedzią na zarzuty innych właścicieli lokali na poświęcanie skarżącej zbyt dużej ilości czasu i zaangażowania zbyt dużych środków w prowadzenie sporów z nią. Miała także wykazać, że nie wspólnota jest inicjatorem tych sporów. Wyjaśniono, że broszurę przygotowano w liczbie adekwatnej do liczby lokali, zaś doręczanie tego rodzaju korespondencji jest uregulowane stosowną uchwałą wspólnoty. Generalny Inspektor zauważył, że niewątpliwie doszło do przetwarzania danych skarżącej, jednak znajdowało ono uzasadnienie w przesłankach legalizujących przetwarzanie tego rodzaju danych osobowych[37]. Wspólnota mieszkaniowa, a tym samym jej członkowie, byli stroną w sporach ze skarżącą toczących się przed sądem lub innymi organami. Ponadto, zgodnie z art. 29 ust. 3 ustawy z dnia 24 czerwca 1994 r. o własności lokali (t.j. Dz. U. z 2015 r., poz. 1892), każdemu właścicielowi lokalu zostało przyznane prawo kontroli działalności zarządu. Każdy członek wspólnoty miał zatem prawo do pozyskania informacji o sposobie ponoszenia wydatków przez wspólnotę związanych z obsługą procesów skarżącej, zwłaszcza wobec domniemań co do niegospodarności zarządu w związku z powyższym[38].

W innej ze spraw zarzut dotyczył podejrzenia nieprawidłowości w roznoszeniu korespondencji przez pracowników, w tym niezabezpieczenia danych (bez koperty)[39]. Choć przepisy nie wskazują na konieczność stosowania specjalnej formy przesyłania korespondencji (np. listem poleconym)[40], to jednak administrator danych osobowych jest zobowiązany do zachowania w poufności jej treści. Jak wskazano, środki zabezpieczenia powinny być adekwatne do zagrożenia, do czego ocenienia zobowiązany jest administrator. Natomiast jednoznacznym wymogiem jest dopuszczenie do przetwarzania danych osobowych wyłącznie osób, które posiadają stosowne upoważnienie nadane przez administratora (art. 37 ustawy). Administrator powinien wziąć również pod uwagę zakresy stosownych upoważnień. Nie wydaje się bowiem konieczne, aby każdy pra-

[36] Decyzja GIODO z 27 lipca 2016 r. (DOLiS/DEC-650/16).
[37] Decyzja GIODO z 7 grudnia 2016 r. (DOLiS/DEC-1308/16).
[38] Patrz również wyrok WSA w Warszawie z 2 lipca 2008 r., sygn. akt. II SA/Wa 2007/07.
[39] Decyzja GIODO z 23 listopada 2016 r. (DOLiS/DEC-1195/16).
[40] Patrz wyrok WSA w Warszawie z 17 czerwca 2004 r. (sygn. akt. II SA/Wa 735/2004).

cownik miał dostęp do wszystkich danych osobowych. Działanie takie może być słusznie kwestionowane. Zakres upoważnienia powinien zatem odzwierciedlać faktyczny zakres dostępu do danych i być adekwatny do pełnionych obowiązków. O ile zatem personel pomocniczy posiada upoważnienie do przetwarzania danych osobowych w związku z doręczaniem korespondencji, o tyle nie wydaje się uzasadnione upoważnienie do zapoznawania się z treścią doręczanych pism. Należy zwrócić uwagę, że tajemnica korespondencji stanowi jedno z dóbr osobistych każdego człowieka chronionych na podstawie art. 23 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t.j. Dz. U. z 2017 r. poz. 459). Administrator powinien rozważyć doręczanie korespondencji co najmniej w zamkniętych kopertach oraz zawężanie stosownych upoważnień do przetwarzania tylko tych danych, których przetwarzanie dla pracy upoważnionych osób jest niezbędne.

Z kolei udostępnienie na walnym zgromadzeniu członkom spółdzielni danych osobowych o wysokości zadłużenia jednego z członków GIODO uznał za uprawnione w świetle art. 23 ust. 1 pkt 5 ustawy[41]. Informacje o zadłużeniu czynszowym członków spółdzielni mieszkaniowej są informacjami bezpośrednio dotyczącymi ich majątku, zatem posiadają faktyczny interes w uzyskaniu takich informacji. Należy jednak zwrócić uwagę, że dostęp do walnego zgromadzenia powinien ograniczyć się wyłącznie do osób uprawnionych do uczestnictwa w nim. W sytuacji gdyby dostęp był otwarty i mogłyby w nim uczestniczyć osoby postronne, udostępnienie danych osobowych w tym zakresie mogłoby zostać uznane za nieprawidłowe. Administrator powinien przedsięwziąć środki w celu zapewnienia dostępu do walnego zgromadzenia tylko osobom uprawnionym. Należy również wziąć pod uwagę, że zakres danych i informacji przekazywanych członkom spółdzielni powinien być adekwatny do potrzeb.

2.8. Oświata i szkolnictwo wyższe

W roku 2016 do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło 49 skarg dotyczących szeroko pojętej oświaty i szkolnictwa.

Sprawy tego rodzaju dotyczą wielu aspektów związanych z życiem w społeczności, które wzajemnie się przeplatają. Chodzi tu zatem o relacje zarówno zachodzące pomiędzy nauczycielem a szkołą, oraz między szkołą, uczniem i rodzicem.

W jednej ze spraw przedmiotem skargi było przetwarzanie danych osobowych w Systemie Informacji o Szkolnictwie Wyższym. Zgodnie z art. 34a ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym[42], minister właściwy do spraw szkolnictwa wyższego prowadzi System Informacji o Szkolnictwie Wyższym w ramach Zintegrowanego Systemu Informacji o Nauce i Szkolnictwie Wyższym „POL-on". System ten pełni rolę ogólnopol-

[41] Decyzja GIODO z 29 listopada 2016 r. (DOLiS/DEC-1253/16).
[42] t.j. Dz. U. z dnia 2016, poz. 1842 ze zm.

skiego wykazu nauczycieli akademickich i pracowników naukowych. Zgodnie zaś z przepisami wykonawczymi, rektorzy uczelni odpowiadają za jakość i aktualność danych w nim zawartych. Generalny Inspektor wskazał w decyzji, że uczelnie są zobowiązane czuwać nad aktualnością danych zawartych w systemie i nie mogą czynności z tym związanych przesuwać w czasie, gdyż prawidłowość tych danych może nieść doniosłe skutki prawne[43]. Niewykreślenie nauczyciela akademickiego z minimum kadrowego danej uczelni, pomimo zakończenia stosunku pracy, uniemożliwia jego zatrudnienie w innej szkole wyższej. Ponadto brak aktualizacji danych może powodować błędną informację co do obsady kadrowej uczelni.

W innej ze spraw w wątpliwość podano udostępnienie danych osobowych skarżącej oraz jej dziecka zawartych w opinii sporządzonej przez wychowawcę klasy na rzecz osoby trzeciej. W sprawie tej okazało się, że opinia jedynie pośrednio dotyczyła dziecka skarżącej, gdyż opisywała relacje między uczniami. Opinia została sporządzona na żądanie rodzica innego ucznia, w celu przedstawienia jej w sądzie w związku z toczącym się postępowaniem. W ocenie Generalnego Inspektora, takie wykorzystanie danych osobowych było właściwe, gdyż znajdowało uzasadnienie w przepisach prawa[44]. Należy bowiem wskazać, że udostępnienie danych osobowych skarżącej oraz jej dziecka miało związek z funkcjonowaniem dziecka w szkole. Wydanie opinii na temat dziecka było realizacją podstawowego prawa rodzica do wykonywania pieczy nad swoim dzieckiem, a organ administracji publicznej, jakim jest szkoła, powinien takiej pomocy rodzicowi udzielać. Bezsprzecznie władza rodzicielska dająca prawo rodzicom do wykonywania pieczy nad dzieckiem rozciąga się również na prawo do pozyskiwania opinii o swoim dziecku, zarówno w kontekście jego rozwoju psychicznego, jak i fizycznego.

[43] Decyzja GIODO z 25 marca 2016 r. (DOLiS/DEC-226/16).
[44] Decyzja GIODO z 10 lutego 2016 r. (DOLiS/DEC-120/16).

2.9. Służba zdrowia.

W 2016 r. zanotowano prawie trzykrotny wzrost skarg w sektorze dotyczącym służby zdrowia w porównaniu z latami poprzednimi (rok 2014 – 47, rok 2015 - 59, rok 2016 - 160).

Do tak istotnego wzrostu przyczyniło się przede wszystkim wpłynięcie kilkudziesięciu skarg (ponad 90) na bezprawne udostępnienie danych osobowych rodziców i ich dzieci na rzecz Państwowego Powiatowego Inspektora Sanitarnego przez osoby przeprowadzające szczepienia ochronne. Powodem złożenia skarg były kierowane przez ww. inspekcję upomnienia wzywające do spełnienia obowiązku szczepiennego w stosunku do małoletniego. Wbrew zarzutom skarżących co do bezprawności takiego udostępnienia kwestia ta została szczegółowo uregulowana w przepisach prawa, statuując legalność takiego udostępnienia i przetwarzania danych osobowych. Jak ustalono w toku postępowań, zgodnie z ustawą z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi[45], osoby przebywające na terytorium Rzeczypospolitej Polskiej są obowiązane na zasadach określonych w tej ustawie do poddawania się szczepieniom ochronnym. W przypadku osoby nieposiadającej pełnej zdolności do czynności prawnych odpowiedzialność za wypełnienie obowiązków ponosi osoba, która sprawuje prawną pieczę nad osobą małoletnią. Państwowy Powiatowy Inspektor Sanitarny sprawuje nadzór w zakresie realizacji obowiązku poddawania się szczepieniom ochronnym, zaś osoby przeprowadzające szczepienia są bezsprzecznie zobligowane do informowania inspekcji o niewypełnieniu ww. obowiązku. Ustawodawca przewidział zarówno uprawnienie inspekcji do pozyskiwania danych osobowych osób nierealizujących obowiązku szczepień, jak również możliwość przetwarzania tych danych w ramach wykonywania nadzoru nad realizacją tego obowiązku. Przekazanie danych osobowych było zatem celowe i adekwatne, ponieważ stanowiło warunek konieczny do wykonania prawa nadzoru inspekcji w zakresie realizacji obowiązku szczepień ochronnych.

Poza tym szczególnym przypadkiem, skargi w związku z szeroko pojętą służbą zdrowia dotyczą przeważnie udostępnienia danych osobowych osobom do tego nieupoważnionym (w tym nieprawidłowego ich zabezpieczenia) oraz zagubienia dokumentacji, jej poszukiwania lub wniosku o nakazanie jej udostępnienia.

Kwestia prowadzenia i udostępniania dokumentacji medycznej została szczegółowo uregulowana w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[46] oraz w rozporządzeniu Ministra Zdrowia wydanym na podstawie delegacji ustawowej zawartej w art. 30 ust. 1 ww.

[45] t.j. Dz.U. z 2016 r., poz. 1866 ze zm.
[46] t.j. Dz.U. z 2016 r., poz. 186 ze zm.

ustawy[47]. Zgodnie z ww. ustawą, pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych[48]. Prawo dostępu do dokumentacji medycznej jest zatem jednym z podstawowych praw pacjenta zapewniającym mu dostęp do informacji o swoim stanie zdrowia. W odróżnieniu od prawa dostępu do dokumentacji medycznej, uprawnienie przewidziane w art. 33 ustawy o ochronie danych osobowych dotyczy informacji o przetwarzanych danych osobowych wnioskodawcy i służy kontroli procesu ich przetwarzania.

Zakres informacji, do których przekazania zobligowany jest administrator danych w związku z wnioskiem osoby, której dane są przetwarzane, został w sposób wyraźny określony w przepisach ustawy, tj. w art. 33 ust. 1 w zw. z art. 32 ust. 1 pkt 1-5 ustawy. Dokumentacja medyczna, jako taka, zawiera zatem niewątpliwie szerszy zakres informacji. Pacjent, wnioskując o swoją dokumentację medyczną, ma bowiem możliwość pozyskania wszystkich informacji w niej zawartych, których co do zasady nie jest uprawniony żądać na podstawie ustawy o ochronie danych osobowych.

Obowiązek informacyjny przewidziany w ustawie o ochronie danych osobowych nie może zatem zastępować w swoim zakresie żądania do uzyskania dokumentacji medycznej. Są to odrębne od siebie uprawnienia, o innym zakresie przedmiotowym, służące różnym celom i realizowane co do zasady w odmienny sposób. Obu uprawnień nie należy zatem utożsamiać.

2.10. Ubezpieczenia społeczne, majątkowe i osobowe

Liczba skarg kierowanych w 2016 do Generalnego Inspektora dotyczących działania sektora ubezpieczeń społecznych, majątkowych i zdrowotnych uległa nieznacznemu zwiększeniu - wpłynęło 75 skarg (2,9% ogółu).

W jednej z takich spraw Generalny Inspektor zwrócił uwagę na obowiązek zachowania przez administratora danych szczególnej staranności wyrażonej w art. 26 ustawy[49]. W szczególności wskazano, że w przypadku powzięcia wątpliwości co do adresu, na który powinna być wysyłana korespondencja do klienta, który zawarł ze spółką kilka umów, administrator danych osobowych jest zobowiązany uprzednio wyjaśnić tę kwestię. Spółka przyjęła, że adres wskazany na ostatniej umowie, jest aktualnym adresem korespondencyjnym, w związku z czym skierowała na ten adres informacje dotyczące pozostałych umów. Jak okazało się w toku postępowania, inny adres wynikał z faktu, że skarżący zawarł jako ubezpieczający, umowę ubezpieczenia mieszkania na rzecz osoby trzeciej, wskazując jako adres korespondencyjny adres właścicieli tego mieszkania.

W innej ze spraw Generalny Inspektor uznał za prawidłowe udostępnienie danych osobowych na rzecz ubezpieczyciela, i w następstwie ich dalsze przetwarzanie, w związku

[47] Obecnie rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t.j. Dz.U. z 2015 r., poz. 2069).
[48] art. 23 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.
[49] Decyzja GIODO z 26 października 2016 r. (DOLiS/DEC-1072/16).

z zawartą umową ubezpieczenia od odpowiedzialności cywilnej[50]. W sprawie tej skarżący skierował wobec ubezpieczonego pozew o ochronę dóbr osobistych. Przetwarzanie danych osobowych skarżącego zgromadzonych w toku postępowania likwidacyjnego w dokumentacji szkodowej miało swoje oparcie w art. 23 ust. 1 pkt 2 ustawy, tj. przetwarzanie danych było dopuszczalne ze względu na ich niezbędność dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

2.11. Telekomunikacja

W rozpatrywanych w 2016 r. sprawach dotyczących telekomunikacji do Biura GIODO wpłynęło 128 skarg (4,9% ogółu) i dotyczyły one przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych.

Aktualnym problemem związanym z działalnością operatorów telekomunikacyjnych, który w 2016 r. został szczególnie wyeksponowany, jest pozyskiwanie kopii dowodów tożsamości.

Zgodnie z tak zwaną ustawą antyterrorystyczną[51], w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne wprowadzono obowiązek rejestracji telefonicznych kart pre-paid. Spowodowało to wątpliwości co do zakresu zbieranych danych osobowych w związku z realizacją tego obowiązku. Zgodnie z dodanym art. 60b ust. 1 Prawa telekomunikacyjnego, abonent, ze wskazanymi w ustawie wyłączeniami, podaje dostawcy usług imię, nazwisko oraz numer PESEL, jeżeli go posiada, albo nazwę, serię i numer dokumentu potwierdzającego tożsamość. Jednocześnie ustawodawca dopuścił podanie tych danych drogą elektroniczną lub w inny, określony przez niego sposób (art. 60b ust. 2). Należy podkreślić, że określony sposób nie oznacza dowolny.

Co istotne, dowody osobiste oprócz takich danych, jak imię i nazwisko, zawierają również wiele innych, w tym m.in. wizerunek osoby identyfikowanej czy widniejące na starych dowodach, również wzrost i kolor oczu. Wymuszenie przekazania kopii dowodu osobistego prowadzi zatem do pozyskania danych osobowych w poszerzonym, nadmiarowym zakresie, który nie jest wymagany przez przepisy prawa, w związku z powyższym taki sposób pozyskiwania danych nie powinien być stosowany.

W jednej ze spraw, Generalny Inspektor uznał za wątpliwą z punktu zasad ochrony danych osobowych praktykę polegającą na uzależnianiu zawarcia umowy na promocyjnych warunkach od udzielenia przez klientów pisemnej zgody na wykonanie kserokopii dokumentu tożsamości[52]. Generalny Inspektor stwierdził, że spółka nie spełniła przesłanek uprawniających ją do przetwarzania danych osobowych tego klienta w szerszym zakresie. Jedyną okolicznością dającą podstawę do przetwarzania

[50] Decyzja GIODO z 11 listopada 2016 r. (DOLiS/DEC-1248/16).
[51] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2016 r., poz. 904 ze zm.).
[52] Decyzja GIODO z 23 grudnia 2016 r. (DOLiS/DEC-1400/16).

dodatkowych danych, które znajdują się na kopii dowodu osobistego, byłaby zgoda klienta. W niniejszej sprawie spółka nie zagwarantowała jednak warunków umożliwiających złożenie swobodnej oraz dobrowolnej, a tym samym skutecznej zgody na przetwarzanie danych osobowych w zakresie wykraczającym poza przepis art. 161 ust. 2 Prawa telekomunikacyjnego. Nie zapewniono również prawa do wycofania tej zgody w dowolnym czasie.

Zgodnie z Prawem telekomunikacyjnym (art. 57 ust. 1 pkt 3), dostawca usług nie może uzależniać zawarcia umowy o świadczenie publicznie dostępnych usług telekomunikacyjnych od udzielenia informacji lub danych, innych niż określone w tej ustawie (w art. 161 ust. 2). Jednocześnie, chociaż dostawca usług może uzależnić zawarcie umowy o świadczenie usług telekomunikacyjnych od dostarczenia przez użytkownika końcowego dokumentów potwierdzających możliwość wykonania zobowiązania wobec dostawcy usług wynikającego z umowy(z art. 57 ust. 2 pkt 1), to jednak należy zaznaczyć, że kopia dowodu osobistego, jako dokument tożsamości, nie zawiera informacji, które pozwalają na dokonanie takiej oceny[53].

Generalny Inspektor stwierdził, że w tej konkretnej sprawie przetwarzanie przez spółkę danych osobowych znajdujących się w kopii dowodu osobistego, które wykraczają poza dozwolony przepisami zakres, nie znajdowało uzasadnienia na gruncie przepisów ustawy o ochronie danych osobowych i Prawa telekomunikacyjnego i nakazał zaprzestanie przetwarzania danych osobowych klienta znajdujących się w kopii jego dowodu osobistego pozyskanego przez spółkę, w nieadekwatnym zakresie, tj. jego wizerunku oraz danych o wzroście i kolorze oczu.

W przypadku podmiotów telekomunikacyjnych, podobnie jak u innych administratorów z sektora prywatnego, częstym problemem jest również prowadzenie marketingu, mimo złożonego sprzeciwu. Generalny Inspektor ponownie wskazał, że podmiot profesjonalny nie może zasłaniać się błędami pracowników w przypadku nieodnotowywania sprzeciwów na przetwarzanie danych osobowych w celach marketingowych. Kilkukrotne kontaktowanie się z klientami w celu przedstawienia im oferty handlowej, mimo złożonego sprzeciwu, w trakcie trwania umowy, po jej zakończeniu, lub też pomimo faktu potwierdzenia wycofania zgody, należy uznać za uporczywe zaniedbywanie podstawowych obowiązków administratora danych osobowych[54]. Administratorzy powinni podjąć działania mające na celu przeszkolenie pracowników przetwarzających dane osobowe oraz zastosowanie odpowiednich rozwiązań techniczno-organizacyjnych, gwarantujących prawidłową realizację ich obowiązków.

[53] Tak w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 18 lutego 2016 r., sygn. akt II SA/Wa 1655/15, http://orzeczenia.nsa.gov.pl/doc/F6B26720AA (nieprawomocny).
[54] Decyzja GIODO z 11 października 2016 r. (DOLiS/DEC-1001/16).

2.12. Zatrudnienie

W 2016 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło 128 skarg dotyczących przetwarzania danych osobowych w związku z zatrudnieniem.

Problem tzw. ukrytych rekrutacji stał się przedmiotem zainteresowania GIODO w postępowaniu przeprowadzonym z urzędu[55]. Polegają one na publikowaniu ogłoszeń o poszukiwaniu pracownika bez wskazania pracodawcy. Praktyka taka rodzi wątpliwości składających aplikację co do tożsamości podmiotu, który będzie administratorem ich danych osobowych. Na skutek pisma sygnalizującego powyższy problem, Generalny Inspektor w stosunku do podmiotu, który prowadzi stronę internetową i udostępnia narzędzia informatyczne ułatwiające zamieszczanie tego typu ogłoszeń, wszczął postępowanie z urzędu. W sprawie tej uznano, że obowiązek informacyjny wskazany w art. 24 i 25 ustawy nie ciąży na podmiocie oferującym te narzędzia z racji tego, że nie jest administratorem danych osobowych, a procesorem, tj. przetwarza dane osobowe na zlecenie (umowa powierzenia). Wszelkie obowiązki informacyjne ciążą zatem na administratorze danych, czyli potencjalnym pracodawcy.

Generalny Inspektor wskazał również na konieczność analizy przez pracodawców przetwarzanych danych osobowych po ustaniu stosunku pracy. Uznano, że adres e-mail zawierający pierwszą literę imienia oraz nazwisko byłego pracownika w domenie pracodawcy jest daną osobową[56]. Tak skonstruowany adres pozwala jednoznacznie zidentyfikować konkretną osobę powiązaną z danym przedsiębiorcą. Jeżeli adres e-mail został utworzony w ściśle określonym celu, a mianowicie w celu kontaktu pracownika z podmiotami zewnętrznymi, to wobec faktu zakończenia współpracy, pracodawca, jako administrator, powinien dokonać analizy konieczności dalszego przetwarzania tych danych. W tej sprawie Generalny Inspektor wskazał na zawarty w art. 35 ustawy o ochronie danych osobowych obowiązek sprostowania nieaktualnych danych osobowych oraz na zasady celowości i adekwatności przetwarzania danych osobowych wyrażone w art. 26 ustawy. Obowiązkiem administratora było niezwłoczne zaprzestanie przetwarzania danych po ustaniu celu, dla którego te dane były zebrane i wykorzystywane.

W jednej ze spraw skarżący zakwestionował celowość sporządzania przez spółkę notatek służbowych[57]. Rozpatrując ją, GIODO uznał, że przetwarzanie danych osobowych skarżącego w dokumentacji zbieranej w czasie trwania stosunku pracy, w szczególności w sporządzanych notatkach służbowych, miało miejsce na podstawie art. 23 ust. 1 pkt 5 ustawy i jako takie było prawnie dopuszczalne. Spółka niewątpliwie ma prawo weryfikować działania pracowników i dokumentować je w formie notatek służbowych.

[55] Decyzja GIODO z 13 września 2016 r. (DOLiS/DEC-860/16).
[56] Decyzja GIODO z 2 września 2016 r. (DOLiS/DEC-813/16).
[57] Decyzja GIODO z 15 grudnia 2016 r. (DOLiS/DEC-1344/16).

2.13. Windykacja

W 2016 r. zanotowano nieznaczny wzrost liczby skarg na działalność podmiotów zajmujących się windykacją (2014 r. – 110, 2015 r. – 110, 2016 r. – 131). Stanowiły one 5% ogółu.

Skargi z tej kategorii dotyczą głównie legalności pozyskania i dalszego wykorzystywania danych osobowych. Obecnie to często forma podejmowania działań windykacyjnych, a nie podstawa dochodzenia wierzytelności przez dany podmiot, budzi największe zastrzeżenia skarżących[58].

Przetwarzanie danych osobowych w celach windykacyjnych, z punktu widzenia przepisów dotyczących ochrony danych osobowych, związane jest głównie z dwoma przypadkami, tj. gdy jest ono podejmowane przez samego administratora danych (wierzyciela), gdy przetwarzania dokonuje inny podmiot na podstawie stosownej umowy z administratorem (umowy powierzenia)[59]. Sam fakt powierzenia przetwarzania danych osobowych nie musi być komunikowany podmiotowi danych i jego skuteczność nie jest zależna od udzielenia przez niego zgody.

Wzorem lat poprzednich Generalny Inspektor kontynuował swoją linię orzeczniczą dotyczącą legalizacji przetwarzania danych osobowych przez firmy windykacyjne, w związku z ich działaniami zmierzającymi do zawarcia umowy sprzedaży wierzytelności, jako znajdujących uzasadnienie w prawnie usprawiedliwionym celu administratora danych (art. 23 ust. 1 pkt 5 w zw. z art. 23 ust. 4 pkt 2 ustawy).

Również upublicznienie danych na stronie internetowej służącej do ogłaszania ofert było legalne i znajdowało uzasadnienie w prawnie usprawiedliwionym celu administratora, którym jest dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej[60]. Zdaniem GIODO, udostępnienie na stronie internetowej tylko części danych osobowych, niezbędnych do skonkretyzowania wierzytelności w celu jej sprzedaży, nie może być postrzegane jako naruszenie praw i wolności podmiotu danych. Dłużnik musi bowiem liczyć się z tym, że w związku ze zwłoką w spełnieniu zobowiązania jego prawo do prywatności oraz ochrony danych osobowych może zostać ograniczone[61].

Z kolei w innej sprawie Generalny Inspektor skierował wystąpienie, w którym zwrócił uwagę na konieczność dokładnego uregulowania w umowie powierzenia zakresu przeka-

[58] Kwestia istnienia lub nieistnienia wierzytelności, czy też słuszności i zakresu dochodzonych roszczeń cywilnoprawnych, co wielokrotnie wskazywał Generalny Inspektor oraz sądy administracyjne, nie leży w kompetencji organu ds. ochrony danych osobowych; fundamentalny w tym zakresie wyrok Naczelnego Sądu Administracyjnego z dnia 6 czerwca sygn. akt I OPS 2/05, patrz również wyrok WSA w Warszawie z dnia 6 lipca 2006 r. sygn. akt II SA/Wa 2226/05.

[59] Wyrok WSA w Warszawie z 31 maja 2012 r., sygn. akt II SA/WA 2367/11.

[60] Decyzja GIODO z 20 września 2016 r. (DOLiS/DEC-899/16).

[61] Podobnie w wyroku WSA w Warszawie z 30 listopada 2004 r., sygn. akt II SA/Wa 1057/04.

zywanych danych osobowych na rzecz podmiotu podejmującego się windykacji[62]. Zastrzeżenia organu wzbudził brak wskazania pełnego zakresu danych będących przedmiotem powierzenia. Administrator, konstruując tego rodzaju umowę, powinien wziąć pod uwagę to, jakie dane są konieczne dla prawidłowego jej wykonania (zasada adekwatności). Przekazanie danych osobowych wykraczających poza zakres przewidziany w umowie należy uznać za nieprawidłowe. Wskazanie dokładnych ram powierzenia ma na celu zapewnienie podstawowych gwarancji ochrony danych osobowych oraz ich prawidłowego przetwarzania. Należy zaznaczyć, że prawidłowe i pełne określenie przedmiotu umowy leży w interesie jej stron, ze względu na odpowiedzialność cywilnoprawną na nich ciążącą.

2.14. Związki wyznaniowe

W 2016 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło 45 skarg, w których kwestionowano legalność przetwarzania danych osobowych przez związki wyznaniowe (1,7% ogółu).

Zdecydowana większość z nich dotyczyła powtarzających się rokrocznie skarg na zaniechanie wykonania przez proboszczów parafii rzymskokatolickich obowiązku uaktualnienia danych osobowych w księgach chrztów na podstawie ustawy o ochronie danych osobowych. Zgodnie z ustawą, każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane. W sprawach tych skarżący kierowali do proboszczów parafii oświadczenie o wystąpieniu z Kościoła katolickiego i, najczęściej, wobec braku satysfakcjonującej odpowiedzi, składali skargi do GIODO na niespełnienie obowiązku uaktualnienia danych i dokonania odpowiedniej adnotacji o wystąpieniu ze związku wyznaniowego w księdze chrztu.

Wskazywana przez organ w poprzednim sprawozdaniu niejednolitość linii orzeczniczej sądów administracyjnych w związku z kolejnymi odwołaniami skarżących i proboszczów parafii rzymskokatolickich, została jednak prawdopodobnie wyeliminowana w związku z serią ważnych wyroków Naczelnego Sądu Administracyjnego z lutego 2016 r.[63] Przykładowo, w wyroku z 19 lutego 2016 r.[64], sąd podkreślił, że Generalny Inspektor Ochrony Danych Osobowych, z mocy wyraźnego i niebudzącego wątpliwości interpretacyjnych art. 43 ust. 2 w zw. z ust. 1 pkt 3 ustawy o ochronie danych

[62] Pismo GIODO z 22 kwietnia 2016 r. (DOLiS-440-1084/14/33682/16).
[63] Patrz wyroki Naczelnego Sądu Administracyjnego z 9 lutego 2016 r. o sygn. akt I OSK 2691/15, I OSK 1509/15, I OSK 579/15, I OSK 2585/15, I OSK 3179/15 oraz I OSK 1466/15.
[64] Wyrok NSA z 19 lutego 2016 r., sygn. akt I OSK 3111/14.

osobowych, nie jest władny do rozpatrywania skarg i wydawania decyzji administracyjnych w sprawach wykonania powszechnie obowiązujących przepisów o ochronie danych osobowych w odniesieniu do zbiorów danych osób należących do kościoła, w tym Kościoła Katolickiego. Uznano, że fakt przynależności do związku wyznaniowego, który posiada unormowaną sytuację prawną w Rzeczypospolitej Polskiej, podlega wewnętrznym regulacjom tego związku.

Wskazano jednocześnie, że GIODO nie jest organem kompetentnym do dokonywania oceny skuteczności wystąpienia z kościoła, sprawy tego rodzaju nie mieszczą się w zakresie zadań określonych w art. 12 ustawy. Zdaniem sądu, organ ds. ochrony danych osobowych mógłby uznać, że określona osoba nie jest już członkiem Kościoła Katolickiego, a tym samym skorzystać ze swoich uprawnień, tylko na podstawie stosownego dokumentu wystawionego przez ten kościół, który dokumentowałby, że dana osoba nie jest już jego członkiem (np. wystawiony akt chrztu z adnotacją o wystąpieniu). Przeświadczenie osoby występującej z kościoła o skuteczności swojego oświadczenia nie jest w tej kwestii wystarczające, gdyż nie spełnia ono specjalnej formy przewidzianej w wewnętrznych przepisach kościelnych dla tych czynności. W szczególności, zdaniem sądu, forma ta nie jest utrudniona i nie czyni całej procedury iluzoryczną. W przedmiotowej sprawie, skoro nie przedstawiono organowi stosownego dokumentu o nieprzynależności do związku wyznaniowego, Generalny Inspektor nie mógł skorzystać z przewidzianych przez ustawę kompetencji. Konkludując, sąd stwierdził, że GIODO powinien umorzyć postępowanie o nakazanie przywrócenia stanu zgodnego z prawem jako bezprzedmiotowe. Jednocześnie sąd wskazał, że całkowite porzucenie wiary lub wystąpienie z Kościoła – niezależnie od oceny dopuszczalności tej ostatniej czynności w świetle prawa kościelnego – nie stanowi żadnego uzasadnienia dla zatarcia pewnych faktów z przeszłości – podobnie jak osoba, która zmienia stan cywilny przez rozwód, nie może żądać usunięcia z akt stanu cywilnego dokonanej wzmianki o zawarciu małżeństwa.

Wskutek zmiennego orzecznictwa sądów administracyjnych prowadzone w tych sprawach postępowania przez GIODO, Generalny Inspektor podejmował działania sygnalizujące zaistniały problem rozbieżności w orzecznictwie sądów administracyjnych, celem utrwalenia linii orzeczniczej[65].

W podobnej sprawie dotyczącej innego związku wyznaniowego skarżący zażądał m.in. usunięcia danych osobowych ze zbioru związku, ze względu na to, że już do niego nie należy[66]. Generalny Inspektor podkreślił, że nie jest uprawniony do oceny przynależności do związku wyznaniowego, jednak w postępowaniu obie strony, zarówno skarżący, jak i związek, potwierdziły fakt obecnej nieprzynależności skarżącego do związku wyznaniowego. W decyzji Generalny Inspektor uznał, że dane osobowe przetwarzane przez związek, przez które należy rozumieć informacje dotyczące członkostwa skarżącego, mają walor historyczny i stanowią dowód jego działalności religijnej. Fakt wystąpienia ze związku nie powoduje, że zebrane dane stają się zbędne do realizacji tego celu, dla którego zostały zebrane. Dane te są niezbędne do celów statutowych związku i znajdują podstawę

[65] Pismo GIODO z 6 maja 2016 r. (DOLiS-072-45/14/38762/16).
[66] Decyzja GIODO z 16 grudnia 2016 r. (DOLiS/DEC-1348/16).

prawną w ustawie o gwarancjach wolności sumienia i wyznania oraz ustawie o narodowym zasobie archiwalnym i archiwach[67].

2.15. Inne

Jedna z organizacji nadająca uprawnienia instruktorskie poinformowała na swojej oficjalnej stronie o zawieszeniu członka w wykonywaniu powyższych uprawnień[68]. W następstwie skarżący zwrócił się o usunięcie jego danych osobowych z ww. informacji. Z zebranego materiału dowodowego wynikało, że powodem do opublikowania notatki o zawieszeniu uprawnień skarżącego był fakt posługiwania się informacją o posiadaniu uprawnień instruktorskich w związku z prowadzoną działalnością gospodarczą, pomimo zawieszenia. Ostatecznie Generalny Inspektor uznał, że udostępnienie przez związek danych osobowych skarżącego we wskazanych okolicznościach, znajdowało oparcie w art. 23 ust. 1 pkt 5 ustawy. Działanie administratora należało uznać za prawnie usprawiedliwione, gdyż działał on w celu ochrony swojego dobrego imienia i renomy, a także w celu uprzedzenia potencjalnych klientów o braku autoryzacji dla działań skarżącego przez związek.

W innej ze spraw, skarżący złożył skargę na przetwarzanie danych osobowych przez przedsiębiorcę w związku z przetwarzaniem jego danych osobowych w celach marketingowych oraz niedopełnienie obowiązku informacyjnego. W toku postępowania ustalono, że przedsiębiorca powierzył przetwarzanie danych osobowych w celach marketingowych na podstawie art. 31 ustawy. W uzasadnieniu Generalny Inspektor wskazał, że powierzenie przetwarzania danych osobowych dokonane przez administratora na podstawie umowy powierzenia nie wymaga uzyskania zgody osoby, której dane dotyczą. Odnosząc się natomiast do zarzutu niespełnienia obowiązku informacyjnego realizowanego na wniosek, na podstawie zebranego materiału dowodowego nie można było jednoznacznie stwierdzić, czy z takim wnioskiem skarżący rzeczywiście wystąpił. Choć przepisy ustawy o ochronie danych osobowych nie zastrzegają określonej formy wystąpienia z tego rodzaju wnioskiem, to jednak dla celów dowodowych wskazane jest złożenie go w takiej formie, która umożliwia jego udokumentowanie. Zgłoszenie wniosku ustnie, np. w rozmowie telefonicznej, może z tego względu być niewystarczające, jednak jeżeli nastąpiło, powinno być spełnione przez administratora.

[67] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz.U. z 2015 r., poz. 1446 ze zm.).
[68] Decyzja GIODO z 6 lipca 2016 r. (DOLiS/DEC-579/16).

3. Kontrola zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Nieprawidłowości stwierdzone w toku prowadzonych przez GIODO kontroli dotyczyły przede wszystkim niewłaściwego dopełniania wobec osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 24 ustawy o ochronie danych osobowych. Kontrole niejednokrotnie wykazywały, że obowiązek ten albo nie był w ogóle realizowany, albo był wykonywany w sposób nieprawidłowy ze względu na niepodawanie wszystkich informacji wymaganych przepisami ww. ustawy.

Do dość częstych uchybień należało również niezgłaszanie prowadzonych zbiorów danych osobowych do rejestracji Generalnemu Inspektorowi oraz zbieranie danych osobowych w szerszym zakresie 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 ich zbierania, pozyskiwali od osób, których one dotyczą, dane wykraczające poza katalog określony w tych przepisach.

Administratorzy danych w dalszym ciągu mają także problemy z prawidłowym sformułowaniem treści oświadczeń o wyrażeniu zgody na przetwarzanie danych osobowych, tak aby wyrażona w taki sposób zgoda nie była domniemana lub dorozumiana z oświadczenia woli o innej treści. Analiza treści oświadczeń zebranych w toku kontroli niejednokrotnie wskazywała, że osobom składającym oświadczenie nie została zapewniona swoboda (możliwość wyboru) przy składaniu tych oświadczeń. Do częstych uchybień w tym zakresie należało również łączenie w jednym oświadczeniu zgód na różne cele przetwarzania danych i na rzecz kilku podmiotów, np. poprzez połączenie zgody na przetwarzanie danych osobowych w celach marketingowych ze zgodą na przesyłanie informacji handlowych za pomocą środków komunikacji elektronicznej.

Liczne uchybienia występowały również w procesie przetwarzania danych osobowych przy użyciu systemów informatycznych.

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 danych, a nawet lekceważenia przepisów.

Niepokojące natomiast wnioski wynikają z treści sprawozdań sporządzanych przez administratorów bezpieczeństwa informacji w związku z realizacją sprawdzeń na wniosek Generalnego Inspektora. Wskazują one na niepełną wiedzę administratorów bezpieczeństwa informacji w zakresie

ochrony danych osobowych niezbędną do prawidłowego sporządzenia sprawozdania ze sprawdzenia, w szczególności w zakresie zgromadzenia adekwatnych dowodów w stosunku do istniejącego stanu faktycznego. Administratorzy bezpieczeństwa informacji częst wskazywali w sprawozdaniach, iż nie stwierdzili nieprawidłowości w procesie przetwarzania danych osobowych, podczas gdy z analizy dokumentacji ze sprawdzeń wynikało, że takie nieprawidłowości miały miejsce. Z informacji przesyłanych przez administratorów bezpieczeństwa informacji wynikało również, iż nie identyfikują w sposób prawidłowy obowiązków ciążących na administratorze danych, np. w przypadku, gdy do przetwarzania danych był wykorzystywany system informatyczny udostępniony przez inny podmiot uznano, że administrator danych nie odpowiada za zabezpieczenie danych osobowych przetwarzanych w tym systemie. Zdarzyło się także, że administrator bezpieczeństwa informacji w związku z wykonanym sprawdzeniem stwierdził, iż podmiot, w którym dokonał sprawdzenia, nie jest administratorem danych przetwarzanych w systemie informatycznym wykorzystywanym do przetwarzania danych osobowych pracowników.

3.1. Kontrole i sprawdzenia

Czynności kontrolne, których celem jest ustalenie, czy jednostka kontrolowana przetwarza dane zgodnie z przepisami o ochronie danych osobowych, przeprowadzane są na podstawie art. 12 pkt 1 i art. 14 ustawy o ochronie danych osobowych. W art. 14 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 kontrolne GIODO.

Uprawnienia te obejmują przede wszystkim 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.

3.2. Kontrola przetwarzania danych osobowych w wybranych obszarach

W 2016 r. przeprowadzonych zostało 147 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Czynnościom kontrolnym poddane zostały m.in. szpitale, banki, komornicy, administracja publiczna.

Większość jednostek kontrolowanych stanowiły podmioty zaliczone do sektora „Inne", obejmującego te podmioty, które ze względu na charakter prowadzonej działalności, nie mogły zostać zakwalifikowane do pozostałych kategorii. Rok 2016 był kolejnym okresem, w którym położony został nacisk na przeprowadzenie tzw. kontroli sektorowych, którymi objęto Policję (11), starostwa powiatowe (10), kancelarie prawnicze (10), izby i urzędy celne (6), wydziały konsularne ambasad RP (4) oraz Straż Graniczną (1). Wyniki przeprowadzonych kontroli obrazują 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 związku z nowelizacją ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922), na mocy której Generalny Inspektor Ochrony Danych Osobowych od 1 stycznia 2015 r. uzyskał uprawnienie zwracania się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c ustawy o ochronie danych osobowych, o dokonanie sprawdzenia określonego w art. 36a ust. 2 pkt 1 lit. a ustawy o ochronie danych osobowych[69], u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia (art. 19b ust. 1 ustawy o ochronie danych osobowych[70]) w **roku sprawozdawczym skierowano 45 wystąpień o dokonanie sprawdzeń przez administratorów bezpieczeństwa informacji**. Wystąpienia o dokonanie sprawdzeń zostały skierowane do banków (20 wystąpień), towarzystw ubezpieczeniowych (10 wystąpień) oraz urzędów miast i gmin (15 wystąpień).

W roku 2016 w związku z przeprowadzonymi kontrolami wydane zostały 44 decyzje administracyjne oraz skierowano 3 zawiadomienia do organów ścigania o podejrzeniu popełnienia przestępstwa określonego w ustawie o ochronie danych osobowych.

W związku ze złożonymi skargami na decyzje wydane na skutek przeprowadzonych kontroli sądy administracyjne wydały dziewięć orzeczeń, w tym siedem orzeczeń wydał Wojewódzki Sąd Administracyjny w Warszawie i dwa Naczelny Sąd Administracyjny.

3.2.1. Administracja publiczna

W 2016 r. w podmiotach wykonujących zadania publiczne z zakresu pobierania cła przeprowadzono 6 kontroli, w tym 4 w izbach celnych, 2 w urzędach celnych oraz u Szefa Służby Celnej [71].

Kontrole obejmowały swoim zakresem przetwarzanie danych osobowych w systemie informacji celnej, ustanowionym na mocy 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 (Dz.U. L 82 z 22.3.1997, str. 1) oraz decyzji Rady 2009/917/WSiSW z dnia 30 listopada 2009

[69] Art. 36a.2.1.a) ustawy o ochronie danych osobowych. 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.

[70] Art. 19b.1 ustawy o ochronie danych osobowych. 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.

[71] Np. kontrole: DIS-K-421/100/16, DIS-K-421/106/16, DIS-K-421/108/16 i DIS-K-421/116/16.

r. w sprawie stosowania technologii informatycznej do potrzeb celnych (Dz. Urz. UE L 323/20).

System informacji celnej jest komponentem systemu informatycznego o nazwie „AFIS" (system informacji w celu zwalczania nadużyć finansowych), udostępnionym do stosowania administracji celnej państw członkowskich Unii Europejskiej przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i służy do rejestrowania ujawnionych przypadków nielegalnego wwozu na teren Unii Europejskiej i wywozu z terenu Unii Europejskiej określonych towarów, np. wyrobów tytoniowych, narkotyków, broni, alkoholu oraz identyfikującą bazą danych rejestru celnego, zawierającą indeks / wykaz prowadzonych postępowań przez służby celne państw Unii Europejskiej oraz inne służby w sprawach celnych i rolnych, w celu zapobiegania działaniom naruszającym przepisy prawa celnego i prawa rolnego mającego zastosowanie do towarów wwożonych na obszar celny Unii Europejskiej lub wywożonych z niego, a także w ułatwianiu i przyspieszaniu ich wykrywania i ścigania. Ma wspierać właściwe organy państw członkowskich Unii Europejskiej w prowadzeniu przez nie postępowań.

Zgromadzony w toku kontroli materiał dowodowy został wykorzystany do przygotowania dla Wspólnego Organu Nadzorczego ds. Celnych odpowiedzi na pytania zawarte w kwestionariuszu dla państw członkowskich Unii Europejskiej, dotyczące sposobu korzystania z systemu informacji celnej przez krajowe organy celne. Ponadto do Szefa Służby Celnej skierowano pismo z informacją o stwierdzonych uchybieniach w procesie przetwarzania danych osobowych przy wykorzystaniu systemu informacji celnej. Na skutek interwencji inspektorów, zostały podjęte przez Szefa Służby Celnej działania, które dały podstawę do uznania, że w zakresie objętym kontrolą przywrócony został stan zgodny z prawem.

W związku z zaleceniem Generalnego Inspektora w zakresie dokumentacji przetwarzania danych osobowych przy wykorzystaniu systemu „AFIS" skierowanych do Szefa Służby Celnej po przeprowadzonej przez inspektorów kontroli w Ministerstwie Finansów opracowana została nowa dokumentacja opisująca sposób przetwarzania danych osobowych w systemie „AFIS", spełniająca wymagania wynikające z przepisów o ochronie danych osobowych. Wskazana dokumentacja została zatwierdzona przez Szefa Służby Celnej i przekazana do stosowania do izb celnych i urzędów celnych. Ponadto system „AFIS" (i system informacji celnej – „CIS") wymieniany jest jako jeden z systemów użytkowanych w izbach celnych i urzędach celnych w dokumentacji opisującej sposób przetwarzania danych osobowych opracowanej przez te podmioty niezależnie od dokumentacji przekazanej przez Ministerstwo Finansów.

W roku 2016 w ramach kontroli sektorowych, Generalny Inspektor Ochrony Danych Osobowych przeprowadził dziesięć kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez starostów jako organów administracji geodezyjnej i kartograficznej wchodzących w skład Służby Geodezyjnej i Kartograficznej w rozumieniu ustawy z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Dz.U. z 2016 r., poz. 1629 ze zm.).

Zakresem kontroli objęto zasady udostępniania przez starostów danych osobowych z ewidencji gruntów i budynków pod kątem ich zgodności z prawem oraz stosowania przy tej formie przetwarzania danych wymaganych przepisami o ochronie danych osobowych zabezpieczeń organizacyjnych i technicznych.

Inspektorzy wykazali potrzebę modyfikacji i uszczegółowienia niektórych zasad, procedur i dokumentów dotyczących procesu przetwarzania danych osobowych. Część starostów zobowiązano do uzupełnienia wniosków o wpisanie zbioru danych osobowych, jakim jest ewidencja gruntów i budynków, do rejestru zbiorów danych osobowych prowadzonego przez GIODO m.in. w odniesieniu do informacji dotyczącej orzeczeń wydanych w postępowaniu administracyjnym lub sądowym, które stanowią podstawę dokonywania zmian w ewidencji gruntów i budynków i są informacjami, o których mowa w art. 27 ust. 1 ustawy (dane szczególnie chronione).

Inspektorzy stwierdzili także uchybienia w procesie udostępniania danych osobowych z ewidencji gruntów i budynków polegające m.in. na: niezastosowaniu środków kryptograficznej ochrony danych przekazywanych na nośnikach optycznych Agencji Restrukturyzacji i Modernizacji Rolnictwa, Wojewódzkim Inspektorom Nadzoru Geodezyjnego i Kartograficznego oraz Agencji Nieruchomości Rolnych (art. 36 ust. 1 ustawy); niespełnieniu wymogów przewidzianych dla polityki bezpieczeństwa, tj. niezawarciu w jej treści wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 2 – 4 rozporządzenia) i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (część B pkt X załącznika do rozporządzenia); braku zapewnienia przez system służący do przetwarzania danych osobowych daty pierwszego wprowadzenia danych do tego systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu (§ 7 ust. 1 pkt. 1 i 2 rozporządzenia); dokumentacja zawierająca dane osobowe właścicieli i władających nieruchomością, na którą składały się m.in. orzeczenia wydane w postępowaniu sądowym lub administracyjnym na podstawie, których dokonywane są zmiany w ewidencji gruntów i budynków, była przechowywana w sposób umożliwiający osobom nieuprawnionym dostęp do danych osobowych, tj. na otwartych regałach (art. 36 ust. 1 ustawy); udostępnianie kopii dokumentów uzasadniających wpisy do bazy danych operatu ewidencyjnego (m.in. orzeczeń wydanych w postępowaniu sądowym lub administracyjnym) bez odnotowania tego faktu w stosownym rejestrze (art. 38 ustawy).

Na skutek działań inspektorów, w starostwach powiatowych, w których stwierdzono uchybienia w zakresie przekazywania danych poza obszar przetwarzania danych, dokumentacja dotycząca przetwarzania danych (tj. polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym), została rozszerzona o sposoby stosowania środków mających na celu zwiększenie bezpieczeństwa danych. Na podstawie przeprowadzonych kontroli wydano także decyzje nakazujące usunięcie stwierdzonych uchybień w celu przywrócenia stanu zgodnego z prawem.

Biorąc pod uwagę ustalenia inspektorów, Generalny Inspektor, wystąpił także do Ministra Spraw Wewnętrznych i Administracji o podjęcie inicjatywy ustawodawczej w celu zmiany przepisów dotyczących ewidencji gruntów i budynków w zakresie jawności numerów ksiąg wieczystych[72].

[72] Minister Spraw Wewnętrznych i Administracji Departament Administracji Publicznej poinformował Generalnego Inspektora, że pismem z 15 września 2016 r. znak: DAP-WN-0749-9/2016/WWP przekazał niniejsze wystąpienie Generalnego Inspektora według właściwości do Ministra Infrastruktury i Budownictwa.

W roku 2016 Generalny Inspektor Ochrony Danych Osobowych zwrócił się również, na podstawie art. 19b ustawy o ochronie danych osobowych, do administratorów bezpieczeństwa informacji w 15 urzędach gminy (miasta), o dokonanie sprawdzenia zgodności przetwarzania przez wójtów (burmistrzów, prezydentów) gmin danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą o ochronie danych osobowych. Zakresem sprawdzeń objęto przetwarzanie danych osobowych przy realizacji wobec kandydatów do pracy w urzędzie gminy (miasta) obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 i art. 25 ust. 1 ustawy o ochronie danych osobowych.

Inspektorzy, oceniając wyniki przeprowadzonych sprawdzeń uznali, iż w zakresie objętym sprawdzeniami w 7 urzędach dane przetwarzane były zgodnie z przepisami o ochronie danych osobowych. Natomiast nieprawidłowości wystąpiły w 4 gminach i polegały na niezrealizowaniu obowiązku informacyjnego wskazanego w art. 24 ust. 1 ustawy, np. obowiązek informacyjny wskazany w art. 24 ust. 1 ustawy był realizowany wobec kandydata do pracy, który przesyła swą aplikację w odpowiedzi na ogłoszenie o naborze na wolne stanowisko urzędnicze, podczas rozmowy kwalifikacyjnej, zaś obowiązek ten powinien być realizowany przed zebraniem danych, np. w ogłoszeniu. W pozostałych przypadkach ze sprawozdania nie wynikało, czy dopełniony był wskazany obowiązek. Dlatego konieczne było doprecyzowanie informacji przez administratorów bezpieczeństwa informacji.

W toku kontroli przeprowadzonej w jednym z urzędów miasta i gminy, której zakresem objęto przetwarzanie danych w związku z rozpatrywaniem indywidualnych spraw obywateli na sesjach rady miejskiej, ustalono, iż nie została opracowana procedura określająca obowiązek przekazywania radnym kopii dokumentów zawierających dane osobowe interesantów urzędu miasta i gminy za pokwitowaniem i rozliczania ich zwrotu. Jednocześnie ustalono, że nie opracowano procedury, z której wynika, że burmistrz miasta i gminy, zastępca burmistrza i inni pracownicy urzędu miasta i gminy, powinni wypowiadać się podczas sesji rady miejskiej odbywających się z udziałem publiczności bez posługiwania się danymi osobowymi interesantów urzędu.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego burmistrz poinformował, iż opracował i wdrożył do stosowania w urzędzie miasta i gminy zarządzenie w sprawie zasad przekazywania radnym materiałów zawierających dane osobowe interesantów oraz przetwarzania informacji zawierających dane osobowe interesantów na sesjach i komisjach rady miejskiej, ustanawiające obowiązek przekazywania radnym materiałów zawierających dane osobowe interesantów urzędu miasta i gminy, za pokwitowaniem odbioru, ewidencjonowania ich zwrotu, a także obowiązek nieposługiwania się podczas posiedzeń rady miejskiej danymi interesantów z uwagi na publiczny charakter posiedzeń rady miejskiej. Wobec powyższego Generalny Inspektor wydał decyzję administracyjną umarzającą postępowanie administracyjne.

W 2016 r. do Generalnego Inspektora Ochrony Danych Osobowych wpłynęła informacja od radnych dotycząca udostępnienia na stronie internetowej Biuletynu Informacji Publicznej (BIP) urzędu miasta protokołu kontroli przeprowadzonej w Miejskim Ośrodku Pomocy Społecznej (MOPS), który zawierał dane osobowe, w tym dane osób, które odbywały staż w MOPS. Przeprowadzona kontrola wykazała nieprawidłowości w procesie przetwarzania danych osobowych, albowiem na stronie internetowej BIP zostały zamieszczone dane oso-

bowe, które powinny zostać zanonimizowane. W związku z tym Generalny Inspektor wszczął wobec prezydenta miasta postępowanie administracyjne. Przedmiotem postępowania były w szczególności uchybienia dotyczące obowiązującej w urzędzie instrukcji postępowania w sprawie udostępniania materiałów w Biuletynie Informacji Publicznej, która nie zawierała postanowień odnośnie anonimizacji danych osobowych znajdujących się w materiałach udostępnianych w BIP. W powołanej instrukcji nie zostały również zawarte postanowienia nakładające na kierowników komórek organizacyjnych urzędu miasta oraz kierowników miejskich jednostek organizacyjnych, przygotowujących materiały do udostępnienia w BIP (np. odpowiedź na interpelację radnych rady miejskiej), obowiązek dokonania weryfikacji, czy w przygotowywanej odpowiedzi na interpelację zostały zawarte dane osobowe. Na tej podstawie Generalny Inspektor uznał, iż administrator danych naruszył art. 36 ust. 1 ustawy o ochronie danych osobowych, gdyż nie określił w tym zakresie środków organizacyjnych mających na celu zapewnienie ochrony przetwarzanych danych osobowych, a w szczególności ich zabezpieczenia przed udostępnieniem osobom nieupoważnionym. Analiza materiału zgromadzonego w toku kontroli wykazała również, że urząd miasta wysyłał odpowiedzi na interpelacje radnych na prywatne adresy poczty elektronicznej radnych. Biorąc pod uwagę fakt, że odpowiedzi na interpelacje radnych mogą zawierać dane osobowe, stwierdzono, że taki proces przetwarzania danych (sposób przekazywania danych radnym) nie zapewnia właściwej ochrony danym osobowym. Przetwarzanie (w tym przypadku przesyłanie) danych osobowych w związku z realizacją czynności (zadań) służbowych powinno być realizowane wyłącznie z wykorzystaniem środków służbowych, określonych przez administratora danych, które zapewniają ochronę danym osobowym przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Wykorzystywana w opisanym powyżej procesie prywatna poczta elektroniczna radnych - w ocenie Generalnego Inspektora - nie dawała gwarancji, że dostęp do przesłanych danych osobowych mają wyłącznie osoby upoważnione, co w konsekwencji stanowi naruszenie obowiązków wynikających z art. 36 ust. 1 ustawy o ochronie danych osobowych. Przeprowadzona kontrola wykazała ponadto, że pracownik urzędu miasta odpowiedzialny za zamieszczanie w BIP odpowiedzi na interpelacje radnych został ostatni raz przeszkolony w zakresie przepisów dotyczących ochrony danych osobowych w 2004 r. Od tego czasu miało miejsce wiele nowelizacji przepisów ustawy o ochronie danych osobowych, które w sposób istotny zmodyfikowały zasady przetwarzania danych osobowych. W ocenie Generalnego Inspektora, ta okoliczność również mogła przyczynić się do wystąpienia incydentu związanego z udostępnieniem w BIP protokołu z kontroli przeprowadzonej w MOPS z niezanonimizowanymi danymi osobowymi. Nadmienić należy, że obowiązek zaznajamiania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych wynika z art. 36a ust. 2 pkt 1 lit. c ustawy o ochronie danych osobowych[73] (w przypadku gdy powołany został administrator bezpieczeństwa informacji) lub art.

[73] Art. 36a. 2 pkt 1 lit. c ustawy o ochronie danych osobowych. Do zadań administratora bezpieczeństwa informacji należy zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.

36b ustawy o ochronie danych osobowych[74] (w przypadku gdy administrator bezpieczeństwa informacji nie został powołany).

Część stwierdzonych przez Generalnego Inspektora uchybień została usunięta jeszcze w czasie trwania kontroli. W instrukcji postępowania w sprawie udostępniania materiałów w Biuletynie Informacji Publicznej skontrolowanego urzędu miasta określono zasady przetwarzania na te potrzeby danych osobowych. Ponadto poinformowano Generalnego Inspektora, że do przewodniczącego rady miejskiej skierowano pismo informujące, że odpowiedzi na interpelacje radnych będą przekazywane wyłącznie na ich służbową pocztę elektroniczną udostępnioną przez urząd miasta. Jednocześnie zapewniano, że pracownik odpowiedzialny za zamieszczenie w BIP urzędowych materiałów zostanie skierowany na szkolenie z zakresu ochrony danych osobowych. Ponieważ do czasu wydania przez Generalnego Inspektora decyzji kończącej postępowanie takie szkolenie nie odbyło się, wydana została decyzja administracyjna nakazująca, aby pracownik odbył je w ciągu 14 dni od dnia, gdy decyzja stanie się ostateczna.

Protokół z kontroli dokonanej w urzędzie miasta przekazano komendzie miejskiej Policji prowadzącej w tej sprawie postępowanie. Odstąpiono natomiast od złożenia wniosku o wszczęcie postępowania dyscyplinarnego wobec pracownika winnego zaistnienia incydentu, z uwagi na ukaranie go karą upomnienia przez pracodawcę.

Generalny Inspektor Ochrony Danych Osobowych powziął z urzędu wiedzę o tym, że jeden z prezydentów miast nie zabezpieczył danych osobowych przed ich udostępnieniem osobom nieupoważnionym, w wyniku czego urzędowe dokumenty miały znajdować się przed budynkiem urzędu, w miejscu dostępnym dla wielu osób. Wobec powyższego, do urzędu miasta kierowanego przez tego prezydenta Generalny Inspektor skierował kontrolę w celu ustalenia stanu faktycznego dotyczącego ww. zdarzenia. Ustalenia dokonane w toku kontroli wykazały, że w urzędzie miał miejsce incydent, który skutkował naruszeniem bezpieczeństwa danych osobowych: worki z odpadami komunalnymi, w których znajdowały kopie dokumentacji należącej do urzędu, nie zostały wywiezione bezpośrednio po zakończeniu sprzątania przez pracowników podmiotu sprzątającego z wnęki przed wejściem do budynku zajmowanego przez ten urząd. Jak ustalono na podstawie wyjaśnień pracowników, a także dokonanych oględzin obrazu z monitoringu, zawiązane worki ze śmieciami znajdowały się przed wejściem do budynku. Nie ulega wątpliwości, że w workach tych nie powinny znajdować się żadne dokumenty urzędowe przetwarzane przez kontrolowany urząd. Na skutek kontroli dokonanej przez inspektorów GIODO, prezydent miasta podjął natychmiastowe działania zmierzające do wyeliminowania podobnych zdarzeń w przyszłości, tj. m.in. pocztą elektroniczną skierowane zostało do wszystkich pracowników urzędu pismo przypominające o zakazie wykonywania kopii dokumentów bez zgody przełożonego (chyba że obowiązek wykonania kopii wynika z procedur czy przepisów prawa). Ponadto zrezygnowano z zawartej umowy o sprzątanie budynków i pomieszczeń zajmowanych przez urząd i zawarto umowę z innym podmiotem. Ochronę osób i mienia w obiektach urzędu zaczęła sprawować straż miejska, a nie jak wcześniej podmiot trudniący się ochroną. Polityka bezpieczeństwa informacji, z którą zapoznali się

[74] Art. 36b ustawy o ochronie danych osobowych. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1, z wyłączeniem obowiązku sporządzania sprawozdania, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, wykonuje administrator danych.

wszyscy pracownicy urzędu i zobowiązali się do jej stosowania, określa m.in. procedury dotyczące sposobu zabezpieczania oraz przekazywania dokumentacji wewnątrz komórek organizacyjnych urzędu i poza urzędem, a także wykonywania kopii tej dokumentacji. Podjęte przez prezydenta miasta natychmiastowe działania zmierzające do wyeliminowania w przyszłości podobnych zdarzeń spowodowały, że Generalny Inspektor Ochrony Danych Osobowych nie skorzystał ze swoich ustawowych uprawnień i nie wszczął postępowania administracyjnego w sprawie.

Biorąc jednak pod uwagę fakt, iż w ww. sprawie prowadzone było postępowanie karne, poczynione w czasie kontroli ustalenia zostały przekazane do prowadzącej postępowanie Prokuratury celem stosownego wykorzystania.

3.2.2. Bezpieczeństwo publiczne

W 2016 r. przeprowadzono kontrole w zakresie funkcjonowania systemów SISII i VIS.

Kontrole przeprowadzono w następujących podmiotach: placówki konsularne przy ambasadach Rzeczypospolitej Polskiej, Urząd ds. Cudzoziemców, Mazowiecki Urząd Wojewódzki, Straż Graniczna, Komenda Główna Policji oraz komendy powiatowe i wojewódzkie Policji (15 kontroli).

Kontrolami objęto dane osobowe przetwarzane przez uprawnione podmioty w związku z dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych SIS i VIS oraz dokonywania wglądu do danych SIS, zgodnie z przepisami 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.).

W placówkach konsularnych dostęp do danych jest realizowany za pośrednictwem systemu instytucjonalnego Ministerstwa Spraw Zagranicznych służącego do wsparcia pracy urzędów konsularnych. System ten umożliwia m.in. sprawdzenie, czy osoba ubiegająca się o wydanie wizy figuruje w SIS II. Obowiązek dokonania ww. sprawdzenia wynika z ustawy o cudzoziemcach, która określa okoliczności uzasadniające odmówienie cudzoziemcowi wjazdu na terytorium Polski, a także wskazuje przyczyny odmowy wydania cudzoziemcowi wizy krajowej. Jedną z tych okoliczności jest fakt istnienia w SIS II wpisu dotyczącego cudzoziemca do celów odmowy wjazdu. Uprawnienie konsula do dokonywania sprawdzeń w SISII, czy osoba ubiegająca się o wydanie wizy została wpisana do Systemu Informacyjnego Schengen wynika również z rozporządzenia (WE) nr 1987/2006. Poprzez system sprawdzane jest również, czy w SISII nie figuruje dokument (dokumenty), którym posługuje się osoba wnioskująca o wydanie wizy, tj. przede wszystkim paszport. Za pośrednictwem instytucjonalnego systemu informatycznego, służącego do informatycznego wsparcia pracy urzędów konsularnych, realizowany jest również dostęp do danych VIS. Do ww. systemu wprowadzane są m.in. wnioski wizowe

składane w placówkach zagranicznych przez osoby ubiegające się o wydanie wizy. W wydziałach i referatach konsularnych ambasad Rzeczypospolitej Polskiej wydawane są wizy krajowe (uprawniające do wjazdu na terytorium Rzeczypospolitej Polskiej i ciągłego pobytu na nim lub do kilku pobytów na tym terytorium następujących po sobie, trwających łącznie dłużej niż 90 dni w okresie ważności wizy) oraz wizy Schengen (uprawniające do wjazdu i pobytu na terytorium państw należących do strefy Schengen przez okres ważności wizy). Wskazany system instytucjonalny umożliwia m.in. sprawdzenie, czy osoba ubiegająca się o wydanie wizy figuruje w SIS II i w wykazie osób niepożądanych na terytorium RP (o którym mowa w art. 434 ustawy o cudzoziemcach), a w przypadku wizy Schengen również, czy nie złożyła wcześniej wniosku o wydanie wizy Schengen oraz przeprowadzenie konsultacji wizowych krajowych i zagranicznych. Do VIS wprowadzane są przede wszystkim dane dotyczące złożonego wniosku. Ww. informacje są następnie uzupełniane o informacje dotyczące wydania wizy, zaprzestania rozpatrywania wniosku wizowego, odmowy wydania wizy, przedłużenia wizy, unieważnienia lub cofnięcia wizy, w zależności od decyzji podjętej przez konsula w wyniku rozpatrywania wniosku o wydanie wizy. Informacje o przysługujących osobie, której dane dotyczą, prawach w związku z przetwarzaniem jej danych osobowych są dostępne również na stronach internetowych ambasad RP, a także na tablicach informacyjnych przy wejściu do ambasad RP.

W związku z koniecznością wyjaśnienia wątpliwości w odniesieniu do realizacji niektórych obowiązków wynikających z przepisów o ochronie danych osobowych, Generalny Inspektor zwrócił się do Ministra Spraw Zagranicznych o złożenie stosownych wyjaśnień. Uzyskane informacje pozwoliły na uznanie, że na skutek działań podjętych przez Generalnego Inspektora, w przeważającej części został przywrócony stan zgodny z prawem, a co do pozostałej – ponownie organ do spraw ochrony danych zwrócił się o przedstawienie obecnej sytuacji.

W toku kontroli w jednostkach Policji inspektorzy ustalili, że dostęp do danych SIS jest realizowany za pośrednictwem systemu instytucjonalnego Policji. Sprawdzenie w celu wglądu do danych SIS odbywa się m.in. w przypadku: zatrzymania osoby, poszukiwania osoby. Funkcjonariusze dokonują wpisu danych SIS w odniesieniu do osób zaginionych, przedmiotów i pojazdów związanych z osobą zaginioną. Natomiast wgląd do danych SIS jest realizowany w przypadku zwrócenia się innych jednostek organizacyjnych Policji lub innych organów, np. sądów, prokuratury, Straży Granicznej w odniesieniu do osób podejrzanych, poszukiwanych i do tymczasowego aresztowania w związku z prowadzonymi postępowaniami, na podstawie listów gończych lub Europejskich Nakazów Aresztowania. W komendach powiatowych i wojewódzkich Policji sprawdzenia danych VIS są dokonywane również poprzez zakładki systemu instytucjonalnego Policji, za pośrednictwem których sprawdzana jest tożsamość posiadacza wizy, autentyczność wizy lub spełnienie warunków wjazdu lub pobytu na terytorium państw członkowskich Unii Europejskiej. Sprawdzenie ma również na celu zidentyfikowanie osoby, która nie spełnia lub przestała spełniać warunki wjazdu lub pobytu na terytorium państw członkowskich Unii Europejskiej. W celu dokonania takiego sprawdzenia wpisywany jest numer dokumentu.

Jak ustalili inspektorzy GIODO w toku czynności kontrolnych, w jednostce Straży Granicznej dostęp do danych SIS jest realizowany w dwojaki sposób: poprzez aplikację WWW SIS (dla użytkowników indywidualnych) oraz poprzez

system instytucjonalny Straży Granicznej (dla użytkowników końcowych). Sprawdzenia danych w SIS realizowane są przede wszystkim w związku z kontrolą legalności pobytu i zatrudnienia cudzoziemców. Nie stwierdzono uchybień w zakresie objętym kontrolą.

W Urzędzie do Spraw Cudzoziemców przeprowadzona została kontrola w konkretnej sprawie cudzoziemca, w związku z wpisem jego danych do SIS II. Dane cudzoziemca zostały wpisane pomimo zmiany przepisów, które stanowiły podstawę do dokonania wpisu. Inspektorzy po dokonaniu weryfikacji ustalili, że nie ma podstaw do przedłużenia terminu obowiązywania wpisu danych ww. osoby w SIS, z uwagi na to, iż wpis został dokonany na podstawie stanu prawnego obowiązującego w dniu wydania decyzji o wydaleniu z terytorium RP, a nie na podstawie stanu prawnego obowiązującego w dniu dokonywania wpisu. W związku ze zmianą od 12 czerwca 2012 r. przepisów ustawy o cudzoziemcach, dane cudzoziemca, który otrzymał decyzję zawierającą orzeczenie o zakazie ponownego wjazdu jedynie na terytoriom RP, zostały wyłączone z przekazania do SIS.

Zgodnie z powołanymi wyżej przepisami bezpośredni dostęp do Wizowego Systemu Informacyjnego jest realizowany poprzez Krajowy System Informatyczny (KSI) w celu dokonywania wpisów danych VIS przez Straż Graniczną, konsula, wojewodę, ministra właściwego do spraw zagranicznych lub Szefa Urzędu do Spraw Cudzoziemców. W toku kontroli przeprowadzonej w Urzędzie do Spraw Cudzoziemców w Warszawie (sygn. akt DIS-K-421/66/15) ustalono natomiast, że Szef Urzędu do Spraw Cudzoziemców nie realizuje uprawnienia wynikającego z art. 5 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Jak wskazano bowiem, do Szefa Urzędu nie należą zadania, których realizacja wiązałaby się z koniecznością dokonywania wpisów danych VIS. Inspektorzy w toku tej kontroli stwierdzili, że w przypadku wydania przez Szefa Urzędu decyzji o przedłużeniu wizy, czynności w zakresie dodawania danych do VIS, wykonuje wojewoda, jako organ właściwy w sprawie przedłużenia wiz Schengen, zgodnie z art. 84 ust. 1 ustawy o cudzoziemcach (wydaje on cudzoziemcowi nową naklejkę wizową podlegającą wpisaniu do VIS).

W toku kontroli przeprowadzonej w Mazowieckim Urzędzie Wojewódzkim w Warszawie (sygn. akt DIS-K-421/13/16) ustalono, że do tej pory nie zdarzyło się, aby Szef Urzędu do Spraw Cudzoziemców uchylił odmowną decyzję Wojewody Mazowieckiego w sprawie przedłużenia wizy Schengen, której naklejka zarejestrowana byłaby w VIS, i orzekł o przedłużeniu takiej wizy. Jednak gdyby taka sytuacja miała miejsce, wówczas wpisu danych do VIS dokonałby Wojewoda Mazowiecki, jako organ właściwy w sprawie przedłużenia wiz Schengen (Wojewoda Mazowiecki zostałby wskazany jako organ, który przedłużył ważność wizy).

Niemniej Generalny Inspektor zwrócił uwagę, że wątpliwości może budzić, czy w ramach określonych w ustawie z dnia z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (Dz.U. z 2016 r., poz. 23 ze zm.) – uprawnień organu wyższego stopnia do wzruszania decyzji organu pierwszej instancji (w niniejszym przypadku – wojewody), Szef Urzędu do Spraw Cudzoziemców rzeczywiście w żadnym stanie faktycznym nie powinien dokonywać wpisów danych VIS (uwzględniając to, że wpisem jest także zmiana lub usunięcie danych umożliwiających właściwym organom identyfikację osoby oraz podjęcie wnioskowanego działania w związku ze zidentyfikowaniem osoby). W szczególności należy wskazać sytuację, gdy Szef Urzędu do Spraw

Cudzoziemców – na podstawie art. 22 ust. 2 ustawy o cudzoziemcach i art. 157 § 1 ustawy Kodeks postępowania administracyjnego w związku z art. 156 § 1 tej ustawy – stwierdza nieważność decyzji wojewody o przedłużeniu okresu ważności wydanej wizy lub okresu pobytu objętego tą wizą.

W związku z tym, że w świetle przywołanych przepisów wątpliwości budziła konieczność posiadania przez Szefa Urzędu do Spraw Cudzoziemców uprawnienia do dokonywania wpisów danych VIS określonego w art. 5 ust. 1 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, Generalny Inspektor Ochrony Danych Osobowych zwrócił się o rozważenie wprowadzenia zmian w przepisach 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.) w zakresie uprawnienia Szefa Urzędu do Spraw Cudzoziemców do dostępu do danych VIS poprzez ograniczenie tego uprawnienia wyłącznie do wglądu do danych VIS.

W związku z funkcjonowaniem systemu informatycznego o nazwie „Eurodac" przeprowadzono w 2016 r. dwie kontrole[75] zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

Zakresem kontroli objęto przetwarzanie przez komendantów komendy powiatowej i wojewódzkiej Policji danych osobowych w związku z występowaniem z wnioskami o porównanie danych daktyloskopijnych z danymi przechowywanymi w systemie Eurodac na potrzeby ochrony porządku publicznego.

Generalny Inspektor Ochrony Danych Osobowych jest krajowym organem nadzorczym, który jest zobowiązany do monitorowania zgodności z prawem przetwarzania danych osobowych przez państwa członkowskie w celach określonych w rozporządzeniu nr 603/2013.

W związku z ww. monitorowaniem i kontrolą prowadzoną na podstawie ww. rozporządzenia, w 2016 r. zostało skierowane pismo do Dyrektora Centralnego Laboratorium Kryminalistycznego Policji z prośbą o wskazanie, czy w 2016 r. wyznaczone organy, o których mowa w art. 5 rozporządzenia nr 603/2013 występowały z wnioskiem o porównanie danych daktyloskopijnych z danymi przechowywanymi w systemie centralnym na potrzeby ochrony porządku publicznego. Na podstawie wyjaśnień otrzymanych od Dyrektora Centralnego Laboratorium Kryminalistycznego Policji zostały zaplanowane w 2016 r. kontrole w jednostkach organizacyjnych Policji, które występowały z wnioskami o porównanie danych daktyloskopijnych z danymi przechowywanymi w systemie Eurodac na potrzeby ochrony porządku publicznego.

[75] Kontrole DIS-K-421/188/16, DIS-K-421/193/16.

3.2.3. Banki i inne instytucje finansowe

W 2016 r. Generalny Inspektor Ochrony Danych Osobowych zwrócił się do administratorów bezpieczeństwa informacji w 20 bankach o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zakresem sprawdzeń objęto przetwarzanie danych osobowych przez banki w zakresie marketingu kierowanego do klientów oraz osób nie będących klientami banku.

Inspektorzy GIODO oceniając wyniki przeprowadzonych sprawdzeń uznali, iż w zakresie objętym sprawdzeniami, nieprawidłowości ujawnione w bankach wynikały ze stosowania wadliwych klauzul zgód na przetwarzanie danych osobowych w celach marketingowych, a w jednym przypadku bank nie legitymował się podstawą prawną przetwarzania w tym celu danych osobowych osób nie będących jego klientami.

Na podstawie informacji zawartych w sprawozdaniach ze sprawdzeń załączonych do nich dowodów, inspektorzy GIODO stwierdzili, iż osiem banków pozyskuje zgodę na przetwarzanie danych osobowych w celach marketingowych, stosując klauzule zawierające łącznie dwie lub więcej z następujących zgód:

- zgodę na przetwarzanie w celach marketingu własnych produktów lub usług;
- zgodę na przetwarzanie w celach marketingu produktów lub usług innych podmiotów;
- zgodę na używanie telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego, o której mowa w art. 172 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2016 r., poz. 1489 z późn. zm.);
- zgodę na otrzymywanie informacji handlowej, o której mowa w art. 10 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2016 r., poz. 1030).

Zgoda na przetwarzanie danych osobowych powinna spełniać wymogi określone w art. 7 pkt 5 ustawy o ochronie danych osobowych, czyli musi być sformułowana w sposób wyraźny i jednoznaczny oraz wyróżniać się spośród innych pochodzących od osoby ją wyrażającej informacji i oświadczeń woli. Niezbędne jest również umożliwienie tej osobie swobodnego wyrażenia woli w kwestii zgody na przetwarzanie jej danych, m.in. poprzez zapewnienie możliwości wyrażenia zgody niezależnie od innych oświadczeń woli.

Zawarcie kilku zgód w treści jednej klauzuli powoduje, iż osoba, która chciałaby wyrazić tylko jedną lub kilka spośród tych zgód, nie ma takiej możliwości, a zatem nie ma swobody w dysponowaniu swoimi danymi osobowymi.

Zgoda na przetwarzanie danych osobowych powinna być zatem wyodrębniona od innych zgód, również tych, które dotyczą używania telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego czy też otrzymywania informacji handlowych. Przemawia za tym również fakt, iż zgodę na używanie telekomunikacyjnych urządzeń końcowych w celu prowadzenia marketingu bezpośredniego i zgodę na otrzy-

mywanie informacji handlowej regulują przepisy odrębne od przepisów ustawy o ochronie danych osobowych, tj. odpowiednio Prawo telekomunikacyjne i ustawa o świadczeniu usług drogą elektroniczną.

Stanowisko dotyczące konieczności wyodrębnienia zgody na przetwarzanie danych osobowych od innych oświadczeń woli podzielane jest również w orzecznictwie sądów administracyjnych. Jak wskazał Naczelny Sąd Administracyjny w wyroku z 10 stycznia 2013 r. (sygn. I OSK 2029/11), w orzecznictwie istnieje zgodność co do tego, że sposób pozyskiwania zgody na przetwarzanie danych umożliwiać powinien świadome i swobodne wyrażenie woli.

Naczelny Sąd Administracyjny podkreślił, iż zgoda na przetwarzanie danych nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania. Strona nie może być przy tym wprowadzona w błąd. Jeżeli zatem oświadczenie woli dotyczyć ma istotnie różniących się celów przetwarzania, zgoda powinna być wyrażona wyraźnie pod każdym z tych celów przetwarzania.

Zastosowana przez banki forma pozyskiwania zgody na przetwarzanie danych osobowych w celach marketingowych, narusza zatem przepisy ustawy o ochronie danych, bowiem decyzja w sprawie wyrażenia wskazanej zgody nie mogła zostać podjęta swobodnie nie miała charakteru samodzielnego. Naruszało to zatem art. 23 ust. 1 pkt 1 ustawy w związku z art. 7 pkt 5 ustawy o ochronie danych osobowych.

Wobec banków, w których stwierdzono stosowanie wadliwych klauzul zgód, wszczęto postępowania administracyjne. Cztery banki usunęły ww. uchybienie w toku prowadzonych postępowań administracyjnych i z tych względów postępowania te zostały umorzone. Wobec trzech innych banków Generalny Inspektor Ochrony Danych Osobowych wydał decyzje nakazujące usunięcie uchybienia poprzez zapewnienie swobody w przedmiocie złożenia przez klientów zgody na przetwarzanie danych osobowych w celach marketingu produktów banku.

Spośród 20 administratorów bezpieczeństwa informacji, którzy dokonali sprawdzenia przetwarzania danych osobowych przez banki w zakresie marketingu kierowanego do klientów oraz osób niebędących klientami banków, tylko jeden z nich stwierdził naruszenie przepisów o ochronie danych osobowych, pomimo iż w wielu przypadkach ustalenia dokonane przez administratorów bezpieczeństwa informacji w toku sprawdzeń dawały podstawę do stwierdzenia takich uchybień.

Nieprawidłowości stwierdzone przez administratorów bezpieczeństwa informacji polegały m.in. na zbyt rzadkim sprawdzaniu w systemie informatycznym, czy klient nie odwołał zgody na przetwarzanie danych osobowych do celów marketingowych lub nie zgłosił sprzeciwu wobec przetwarzania danych osobowych w tych celach, co mogło skutkować skierowaniem telefonicznej oferty marketingowej do osoby, wobec której brak było podstawy prawnej do przetwarzania jej danych osobowych.

Powyższe naruszenia zostały usunięte w terminach określonych przez administratorów bezpieczeństwa informacji w sprawozdaniu.

3.2.4. Służba zdrowia

Do istotnych kontroli przeprowadzonych w tym sektorze, należała kontrola w jednym ze szpitali, przeprowadzona na skutek wniosku Rzecznika Praw Pacjenta.

Rzecznik Praw Pacjenta zasygnalizował Generalnemu Inspektorowi, że pracownicy zakładu opieki zdrowotnej, tj. rejestratorki oraz sekretarki medyczne posiadają bez stosownej podstawy prawnej dostęp do dokumentacji medycznej pacjentów (m.in. historii choroby pacjenta przetwarzanej w postaci tradycyjnej oraz w systemie informatycznym) zawierającej dane osobowe pacjentów.

Zdaniem ww. organu, administrator danych do przetwarzania danych osobowych pacjentów dopuścił osoby nieupoważnione, które w świetle obowiązujących przepisów prawa nie powinny mieć dostępu do tych danych. Jednak, jak ustalono w toku kontroli, rejestratorki medyczne oraz sekretarki medyczne posiadały dostęp do danych osobowych pacjentów na podstawie ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2016 r., poz. 186) oraz upoważnień nadanych przez administratora danych. Mając na uwadze powyższe uznano, że ww. osoby legitymują się podstawą prawną do przetwarzania danych osobowych pacjentów.

W ramach przedmiotowego sektora inspektorzy przeprowadzili również kontrolę szpitala z inicjatywy prokuratury, która prowadząc postępowanie wobec lekarza zatrudnionego w tym szpitalu i podejrzanego o popełnienie czynu zabronionego na szkodę Narodowego Funduszu Zdrowia, uznała za konieczne dokonanie sprawdzenia sposobu zabezpieczenia danych osobowych pacjentów przez ten szpital. Zakresem kontroli przeprowadzonej w szpitalu objęte zostało w związku z tym zabezpieczenie danych osobowych pacjentów od strony organizacyjnej, jak i technicznej. Analiza materiału dowodowego zebranego w tej sprawie wykazała, że szpital nie zastosował środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności nie zabezpieczył danych pacjentów przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Braki w zabezpieczeniach organizacyjnych i technicznych polegały m.in. na: 1) niewdrożeniu do stosowania polityka bezpieczeństwa, o której mowa rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; 2) niezawarciu w polityce bezpieczeństwa wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; 3) przechowywaniu dokumentacji zawierającej dane osobowe pacjentów na otwartych regałach w miejscach, które były dostępne po zakończeniu pracy przez administrację szpitala i które znajdowały

się w bezpośrednim sąsiedztwie z izbą przyjęć. Do miejsc tych mogły zatem mieć dostęp osoby nieupoważnione.

Wobec szpitala została wydana decyzja administracyjna nakazująca usunięcie stwierdzonych w toku kontroli uchybień w procesie przetwarzania danych osobowych.

3.2.5. Towarzystwa ubezpieczeniowe

W 2016 r. GIODO zwrócił się do administratorów bezpieczeństwa informacji (ABI) w 10 towarzystwach ubezpieczeń na życie o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zakresem sprawdzeń objęto przetwarzanie przez towarzystwa ubezpieczeniowe danych osobowych dotyczących stanu zdrowia osób wnioskujących o objęcie umową ubezpieczenia, pozyskiwanych przed zawarciem umowy.

Inspektorzy, oceniając wyniki przeprowadzonych przez ABI sprawdzeń stwierdzili, iż w części z nich jako podstawę prawną przetwarzania danych o stanie zdrowia osób wnioskujących o objęcie ochroną ubezpieczeniową, zarówno w ramach ubezpieczeń indywidualnych, jak i grupowych, wskazano art. 27 ust. 2 pkt 1 ustawy o ochronie danych osobowych - od osób wnioskujących o zawarcie umowy ubezpieczenia pobierane są pisemne zgody na przetwarzanie danych osobowych w celu oceny ryzyka ubezpieczeniowego oraz zawarcia i wykonania umowy.

Ponadto na wnioskach o zawarcie umowy ubezpieczenia znalazły się klauzule zgód dotyczących:

- uzyskiwania informacji od podmiotów świadczących usługi medyczne, o której mowa w ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2015 r., poz. 1844 z późn. zm.),
- udostępnienia danych osobowych przetwarzanych w zakresie potrzebnym do oceny ryzyka ubezpieczeniowego innym zakładom ubezpieczeń,
- pozyskiwania od Narodowego Funduszu Zdrowia danych o świadczeniodawcach, którzy udzielili świadczeń opieki zdrowotnej osobie wnioskującej o ubezpieczenie.

Ww. klauzule nie stanowiły odrębnych oświadczeń woli osoby, której dane dotyczą. Nie zapewniono również opcjonalności każdego z tych oświadczeń, a zawarcie umowy ubezpieczenia nie było możliwe bez ich akceptacji.

3.2.6. Zatrudnienie

W 2016 r. została przeprowadzona kontrola w jednej z agencji pracy tymczasowej, która przetwarza dane osobowe kandydatów na pracowników tymczasowych m.in. jako podmiot działający na zlecenie innej agencji zatrudnienia.

Ustalono, że umowa powierzenia przetwarzania danych osobowych została zawarta z podmiotem, którego działalność gospodarcza uległa zawieszeniu. Cel powierzenia wskazano w tej umowie ogólnie - jako rekrutowanie kandydatów na pracowników tymczasowych.

Zgodnie z ustawą z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2015 r., poz. 584 ze zm.), przedsiębiorca niezatrudniający pracowników może zawiesić wykonanie działalności gospodarczej na okres od 30 dni do 24 miesięcy. W okresie zawieszenia wykonywania działalności gospodarczej przedsiębiorca nie może wykonywać działalności gospodarczej i osiągać bieżących przychodów z pozarolniczej działalności gospodarczej. W okresie zawieszenia działalności gospodarczej przedsiębiorca ma prawo wykonywać wszelkie czynności niezbędne do zachowania lub zabezpieczenia źródła przychodów.

W związku z tym uznano, że przedsiębiorca może w okresie zawieszenia działalności gospodarczej powierzyć przetwarzanie danych osobowych wyłącznie w celu ich przechowywania i odpowiedniego zabezpieczenia. Ustalenia dokonane w toku opisywanej kontroli wykazały jednak, że podmiot kontrolowany nie tylko przechowywał i zabezpieczał powierzone mu dane, ale także wykorzystywał je we własnym celu, tj. przetwarzał dane w celu rekrutowania kandydatów do pracy tymczasowej w ramach własnej działalności agencji zatrudnienia. Z tego powodu wobec agencji zostało wszczęte postępowanie administracyjne oraz została wydana decyzja administracyjna nakazująca usunięcie opisanych powyżej uchybień.

3.2.7. Transport

Jedną z ciekawszych spraw dotyczących tego sektora była kontrola przeprowadzona w jednym z zarządów komunikacji miejskiej.

Zakresem kontroli objęto dane osobowe przetwarzane w związku z funkcjonowaniem systemu monitoringu w środkach komunikacji miejskiej.

W toku kontroli inspektorzy ustalili, iż w związku z organizowaniem komunikacji miejskiej na terenie miasta i gmin ościennych, podmiot ten podpisuje umowy z przewoźnikami, tj. spółkami transportowymi (komunalnymi i prywatnymi), dotyczące świadczenia usług przewozowych w zakresie lokalnego transportu zbiorowego.

W ramach realizacji tych umów strony uzgodniły między sobą, że administratorem danych osobowych przetwarzanych w zakresie zbiorów danych pochodzących z systemów monitoringu zainstalowanych w pojazdach, będzie przewoźnik, natomiast zarząd komunikacji miejskiej, będący jednostką budżetową miasta, będzie podmiotem, o którym mowa w art. 31 ustawy o ochronie danych osobowych, tj. podmiotem, któremu administrator danych powierzył przetwarzanie danych osobowych.

Z analizy treści umów zawartych pomiędzy przewoźnikami a zarządem komunikacji miejskiej wynikało m.in., że zarząd komunikacji miejskiej zleca przewoźnikom świadczenie usług (tj. przewozów wykonywanych przez przewoźnika na warunkach określonych w umowie oraz zgodnie z obowiązującymi przepisami prawa usług publicznych w zakresie lokalnego transportu zbiorowego przy zachowaniu wymaganych parametrów jakościowych i ilościowych) „w okresie powierzenia" (tzn. w okresie od dnia do dnia, w czasie którego przewoźnik będzie świadczyć usługi na rzecz zarządu komunikacji miejskiej na podstawie umowy) w zamian za rekompensatę, a przewoźnik zobowiązał się wykonać usługi „w okresie powierzenia" na warunkach określonych w uchwałach, umowie oraz zgodnie z obowiązującym prawem. Zarząd komunikacji miejskiej prowadzi bieżący monitoring i kontrolę świadczonych usług zgodnie z zasadami określonymi w umowie.

Ponieważ zarząd komunikacji miejskiej nie realizuje zadań ww. przewoźników w związku z przetwarzaniem danych osobowych zbieranych poprzez monitoring zainstalowany w pojazdach, nie miała w tym przypadku zastosowania instytucja powierzenia przez przewoźników przetwarzania danych zarządowi komunikacji miejskiej, o której mowa w art. 31 ustawy o ochronie danych osobowych. Natomiast instytucja ta ma zastosowanie w przypadku powierzenia przetwarzania danych przewoźnikom przez zarząd komunikacji miejskiej, bowiem przewoźnicy zbierają dane osobowe przy użyciu monitoringu dla realizacji celów zarządu komunikacji miejskiej, np. rozpatrywania przez ten podmiot skarg.

W związku z tym brak było podstaw do zawierania umów powierzenia przetwarzania danych osobowych pomiędzy ww. przewoźnikami, jako administratorami danych osobowych zbieranych poprzez system monitoringu zainstalowany w pojazdach, a zarządem komunikacji miejskiej jako podmiotem, któremu powierzono przetwarzanie tych danych.

Na podstawie całości materiału dowodowego w sprawie uznano, że status administratora danych przetwarzanych w ramach systemu monitoringu dla celu kontroli jakości świadczonych usług (w tym m.in. prowadzenia postępowań skargowych i windykacyjnych) należy przyznać zarządowi komunikacji miejskiej, bowiem on decyduje o celach i środkach przetwarzania danych w ramach tego systemu. Zarząd komunikacji miejskiej przetwarza ww. dane na podstawie art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych, a przewoźnikom zleca wykonanie usług przewozowych i nadzoruje ich realizację. Jednocześnie, w ramach swoich zadań wykonuje m.in. kontrolę świadczonych usług, kontrolę biletów i nalicza opłaty dodatkowe,

rozpatruje skargi, co wiąże się z wykorzystywaniem zapisów z systemu monitoringu. Ponadto powierza przewoźnikom na warunkach określonych w umowach, o których mowa w art. 31 ustawy, gromadzenie danych w ramach tego systemu, określa przy tym cel i zakres przetwarzania tych danych oraz środki, jakie powinny być użyte do przetwarzania danych.

Niezależnie od powyższego status administratora danych przetwarzanych w ramach systemu monitoringu, dla realizacji własnych celów każdego przewoźnika związanych z bezpieczeństwem i ochroną osób i mienia, przyznano także poszczególnym przewoźnikom, którzy przetwarzają te dane na podstawie art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych.

Wobec powyższego w sprawie tej uznano, że w procesie przetwarzania danych występuje wielu administratorów danych osobowych (tj. Zarząd komunikacji miejskiej i poszczególni przewoźnicy), z czego każdy administrator danych realizuje własne cele na przetwarzanych danych, na różnych podstawach prawnych.

Co więcej, w toku kontroli ustalono, że informacja o zainstalowanym monitoringu jest umieszczana na każdym pojeździe przy wejściach zgodnie z zarządzeniem dyrektora zarządu komunikacji miejskiej. W świetle wymogów art. 24 ust. 1 ustawy o ochronie danych osobowych, poinformowanie wyłącznie o fakcie monitorowania uznano za niewystarczające. Zasadne było umieszczenie odpowiednich informacji np. w przepisach porządkowych regulujących korzystanie z komunikacji miejskiej (dostępnych na stronach internetowych i w samych pojazdach) oraz umieszczenie na piktogramach lub obok nich co najmniej nazw administratorów danych i kontaktu (adresu strony internetowej, nr telefonu), za pośrednictwem którego taki obowiązek zostałby spełniony, bowiem osoby, których dane dotyczą, powinny być świadome faktu prowadzenia takiego rodzaju monitoringu. Są to bowiem niewątpliwie działania ingerujące w prawo do prywatności takich osób[76].

Ww. podmiot opracował m.in. wzór nowego piktogramu, który informuje, kto jest administratorem danych gromadzonych w ramach systemu monitoringu, wraz ze wskazaniem pełnych nazw i adresów siedzib oraz danych kontaktowych (nr telefonu wraz z adresem strony www administratora danych), umieszczono także informacje wynikające z art. 24 ust. 1 ustawy o ochronie danych osobowych na stronie internetowej zarządu komunikacji miejskiej.

[76] Opinia 4/2004 Grupy Roboczej Art. 29 z 11 lutego 2004 r. w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer wideo

3.2.8. Internet

W toku kontroli przeprowadzonej w jednej ze spółek, prowadzącej m.in. sklep internetowy, zakresem objęto realizację zadań administratora bezpieczeństwa informacji na podstawie umowy outsourcingu.

Generalny Inspektor uznał, że administrator bezpieczeństwa informacji nie w pełni realizuje zadania określone w ustawie. Administrator bezpieczeństwa informacji powołany przez spółkę, wykonując obowiązek polegający na nadzorowaniu opracowania i aktualizowania dokumentacji przetwarzania danych osobowych, nie dokonał weryfikacji kompletności dokumentacji przetwarzania danych. Jak ustalono w toku kontroli, dokument stanowiący politykę bezpieczeństwa w spółce, nie spełniał wymogów rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), ponieważ: w wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, nie zostały zawarte informacje o lokalizacji serwera, na którym umieszczony jest sklep internetowy spółki, zaś w wykazie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych nie wskazano wykorzystywanych do przetwarzania danych w zbiorze danych programów.

W odpowiedzi na zawiadomienie o wszczęciu postępowania spółka poinformowała, iż uzupełniono politykę bezpieczeństwa w wymaganym zakresie. W związku z tym Generalny Inspektor umorzył postępowanie w niniejszej sprawie.

W związku ze skierowanym do GIODO wnioskiem Rzecznika Praw Dziecka czynności kontrolne zostały przeprowadzone w podmiocie prowadzącym serwis internetowy dla uczniów szkół podstawowych, w ramach którego został przeprowadzony konkurs internetowy. W celu wzięcia w nim udziału należało zarejestrować się na stronie serwisu, podając następujące dane osobowe: imię, nazwisko, adres zamieszkania, nr PESEL, nazwę szkoły, klasę, adres poczty elektronicznej. Wątpliwości Rzecznika Praw Dziecka budziło pozyskiwanie nr PESEL od użytkowników serwisu na potrzeby konkursu jako informacji nieadekwatnej do celu przetwarzania. Analiza materiału dowodowego zebranego w sprawie wykazała jednak, że podmiot legitymował się podstawą prawną przetwarzania danych osobowych użytkowników serwisu, tj. zgodą wyrażoną w treści formularza rejestracyjnego oraz uprawnieniem wynikającym z ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, zgodnie z którym usługodawca może przetwarzać nr PESEL usługobiorcy. Mając na uwadze powyższe uznano, że usługodawca legitymował się podstawą prawną do przetwarzania danych dotyczących nr PESEL użytkowników serwisu, w ramach którego został przeprowadzony konkurs internetowy. Zatem nie można było uznać, że przetwarzanie nr PESEL przez podmiot prowadzący serwis internetowy jest nieadekwatne do celu, w jakim są zbierane dane osobowe.

3.2.9. Kancelarie prawne

W roku sprawozdawczym przeprowadzono kontrole w wybranych 10 kancelariach prawnych.

Kontrole przeprowadzono w 2 kancelariach prowadzonych przez adwokatów, 6 kancelariach prowadzonych przez radców prawnych i 2 kancelariach prowadzonych w formie spółki z ograniczoną odpowiedzialnością. Zakresem tych kontroli objęto zabezpieczenie oraz udostępnianie przez kancelarie prawne danych osobowych klientów.

Czynności kontrolne przeprowadzone w kancelariach prawnych wykazały w zakresie objętym kontrolą nieprawidłowości w procesie przetwarzania danych osobowych, które polegały na nieodpowiednim zabezpieczeniu danych, braku niezbędnych elementów dokumentacji przetwarzania danych, a także na niezawarciu stosownych umów z podmiotami, którym powierzono przetwarzanie danych osobowych. Jednak większość skontrolowanych podmiotów podjęła skuteczne działania mające na celu przywrócenie stanu zgodnego z prawem. Wyeliminowanie uchybień stwierdzonych w toku przeprowadzonych kontroli doprowadziło do sytuacji, w której w przeważającej liczbie skontrolowanych kancelarii zabezpieczenie danych osobowych jest obecnie prawidłowe.

Kontrole wykazały ponadto, iż osiem (8) z dziesięciu skontrolowanych kancelarii naruszyło przepisy ustawy o ochronie danych. Stwierdzone uchybienia polegały m.in. na: niezabezpieczeniu danych osobowych przesyłanych w plikach w formacie DOC i PDF za pośrednictwem skrzynki poczty elektronicznej przed ich udostępnieniem osobom nieupoważnionym; pliki nie były zabezpieczone przed otwarciem; niezawarciu w polityce bezpieczeństwa informacji o podmiotach, na serwerach których utrzymywana jest poczta elektroniczna oraz o podmiocie, na serwerach którego są zlokalizowane dane przetwarzane w aplikacji; nietworzeniu kopii zapasowych plików zawierających dane osobowe, które są przetwarzane na komputerach użytkowanych w kancelarii; niezawarciu z podmiotem, na serwerach którego utrzymywana jest poczta elektroniczna kancelarii, umowy powierzenia przetwarzania danych osobowych; niezawarciu z podmiotem serwisującym system informatyczny umowy powierzenia przetwarzania danych osobowych; niezabezpieczeniu dysku sieciowego zawierającego dane osobowe klientów kancelarii przed dostępem osób nieupoważnionych oraz przed zabraniem przez osobę nieuprawnioną - dysk sieciowy znajdował się w niezamykanej na klucz szafie ustawionej w korytarzu, w którym przebywają osoby postronne.

Na podstawie dokonanych ustaleń stwierdzono, że uchybienia, w szczególności dotyczące dokumentacji przetwarzania danych osobowych oraz bezpieczeństwa danych osobowych zostały niezwłocznie usunięte przez większość skontrolowanych kancelarii i wobec tego nie wszczęto wobec tych podmiotów postępowania administracyjnego. Natomiast wobec kancelarii prawnych, w których stwier-

dzono naruszenie przepisów o ochronie danych osobowych, wszczęte zostały postępowania administracyjne w celu przewrócenia stanu zgodnego z prawem.

3.3. Systemy informatyczne służące do przetwarzania danych osobowych

W ramach przeprowadzonych w 2016 r. kontroli, weryfikacji poddano 532 systemy informatyczne (z czego 369 w ramach oceny sprawozdań ze sprawdzeń).

Liczby poddanych weryfikacji systemów informatycznych w latach 2013 - 2016 r. były następujące:

rok 2013 – 280

rok 2014 – 338

rok 2015 – 258

rok 2016 – 532 (w tym 369 w ramach oceny sprawozdań ze sprawdzeń)

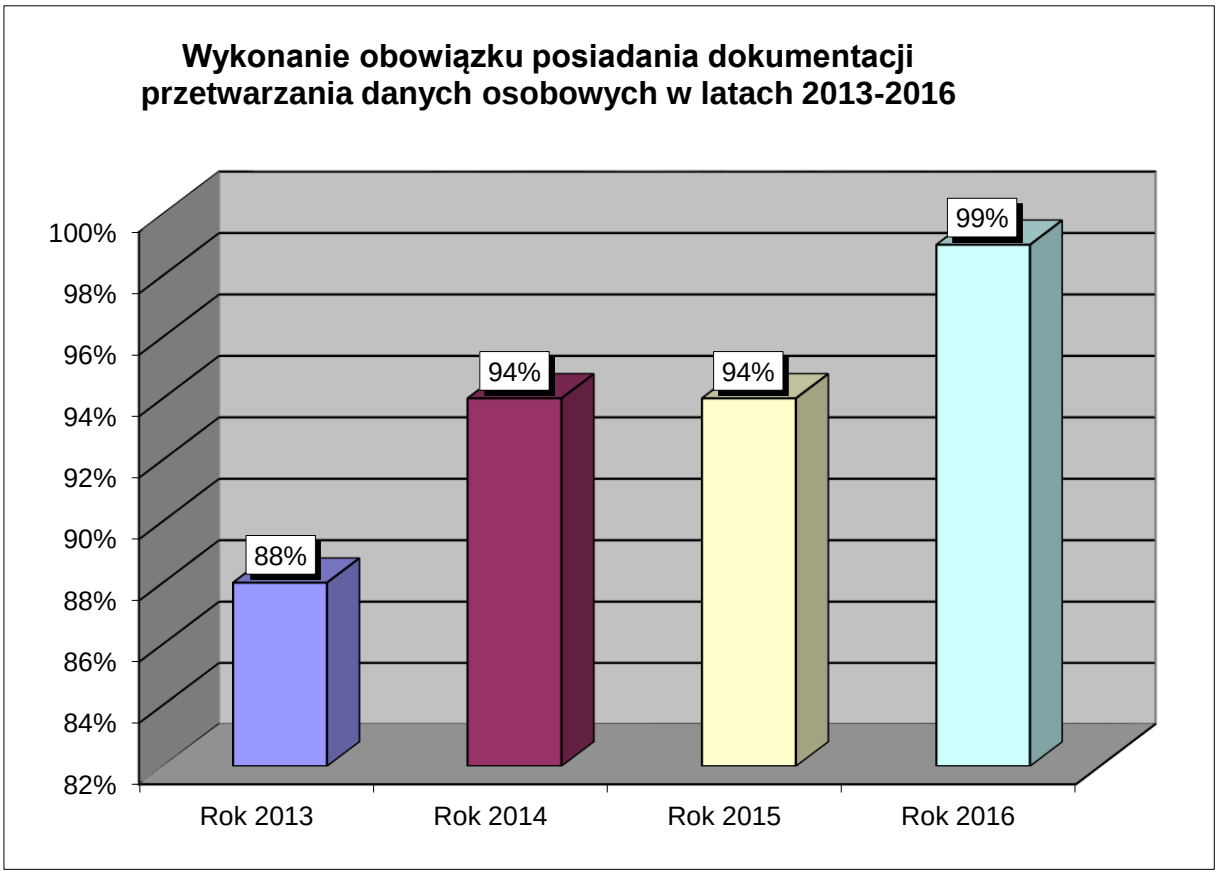
3.4. Wyniki kontroli

3.4.1. Ogólna ocena wyników kontroli w zakresie wypełnienia obowiązków formalnych i organizacyjnych

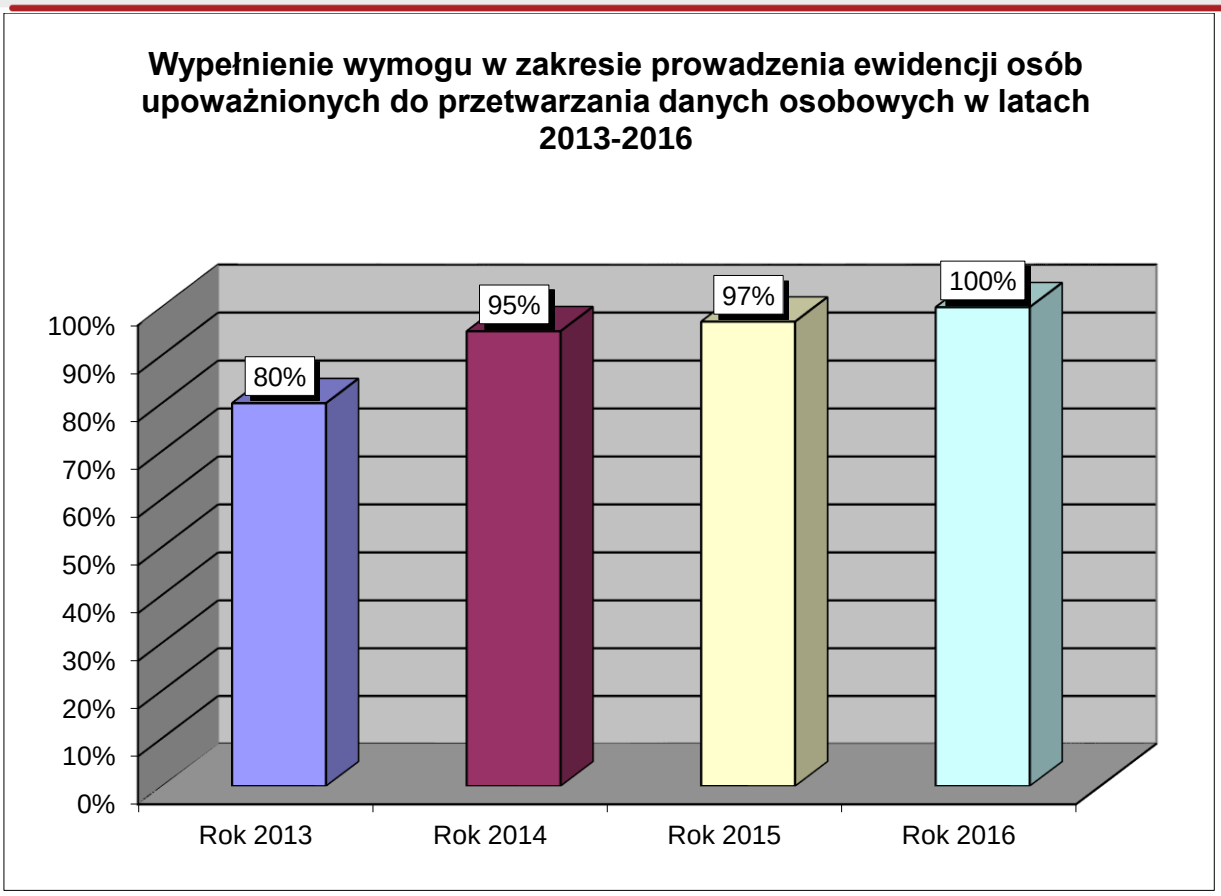
Spełnienie przez kontrolowane podmioty w latach 2013-2016 wymogów formalnych, organizacyjnych i technicznych, o których mowa w ustawie i rozporządzeniu, zobrazowane zostało poniżej w formie wykresów. Pokazują one procentowe wyniki kontroli w odniesieniu do ogólnej liczby kontroli w danym roku lub ogólnej liczby kontrolowanych w danym roku systemów informatycznych. Zamieszczone informacje odnoszące się do prowadzonej dokumentacji procesu przetwarzania danych, obowiązku prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oceniano w skali procentowej w stosunku do liczby kontrolowanych podmiotów. Natomiast warunki odnoszące się do wymagań funkcjonalnych, jakie powinny posiadać systemy informatyczne, oceniane były w skali procentowej do liczby systemów objętych kontrolą.

W przypadku, gdy kontrolowana jednostka opracowała wymagane dokumenty (takie jak polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych), prowadziła ewidencję osób upoważnionych do przetwarzania danych osobowych oraz wdrożyła opisane w dokumentacji procedury przetwarzania danych osobowych w zakresie wymogów formalno-organizacyjnych, realizację wymogu prowadzenia dokumentacji uznawano za prawidłową. Sprawdzano również, czy wyznaczony został administrator bezpieczeństwa informacji oraz czy osoby dopuszczone do przetwarzania danych posiadały stosowne upoważnienia nadane przez administratora danych.

Stopień wypełnienia przez kontrolowane podmioty ww. warunków w latach 2013-2016 przedstawiono na poniższych wykresach.



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



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

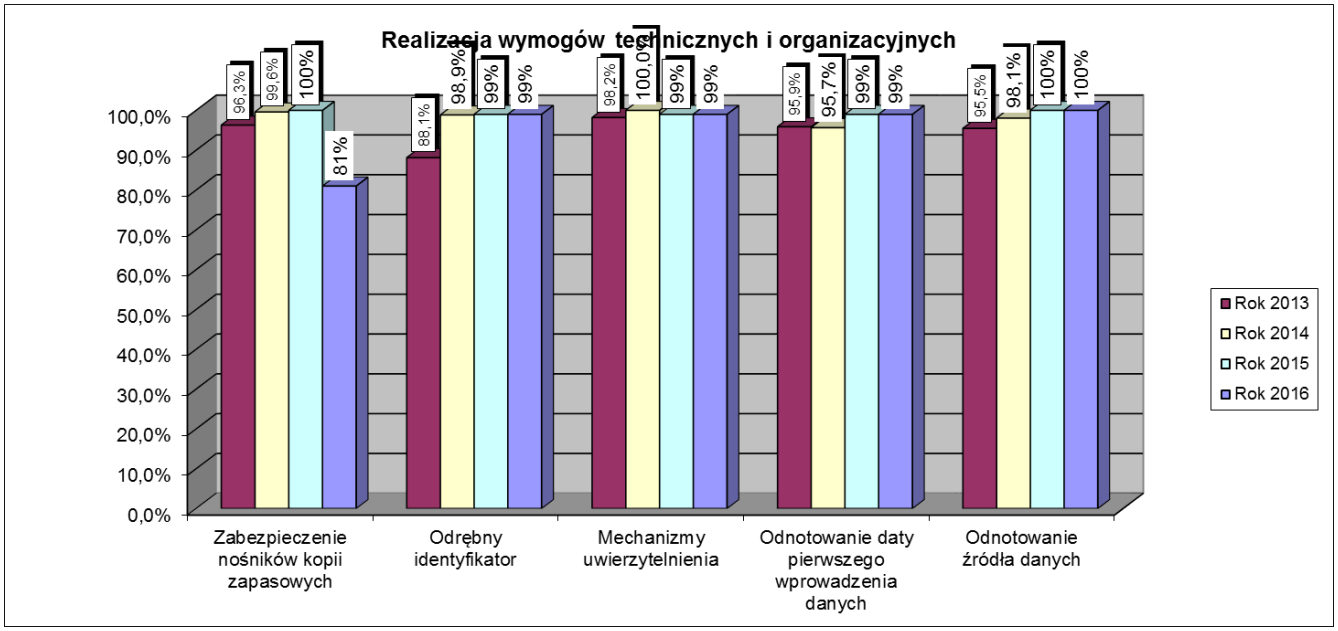
3.4.2. Ogólna ocena wyników kontroli w zakresie warunków techniczno-organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych.

W roku 2016 ocenie zgodności z przepisami o ochronie danych osobowych poddano 532 systemy informatyczne służące do przetwarzania danych osobowych.

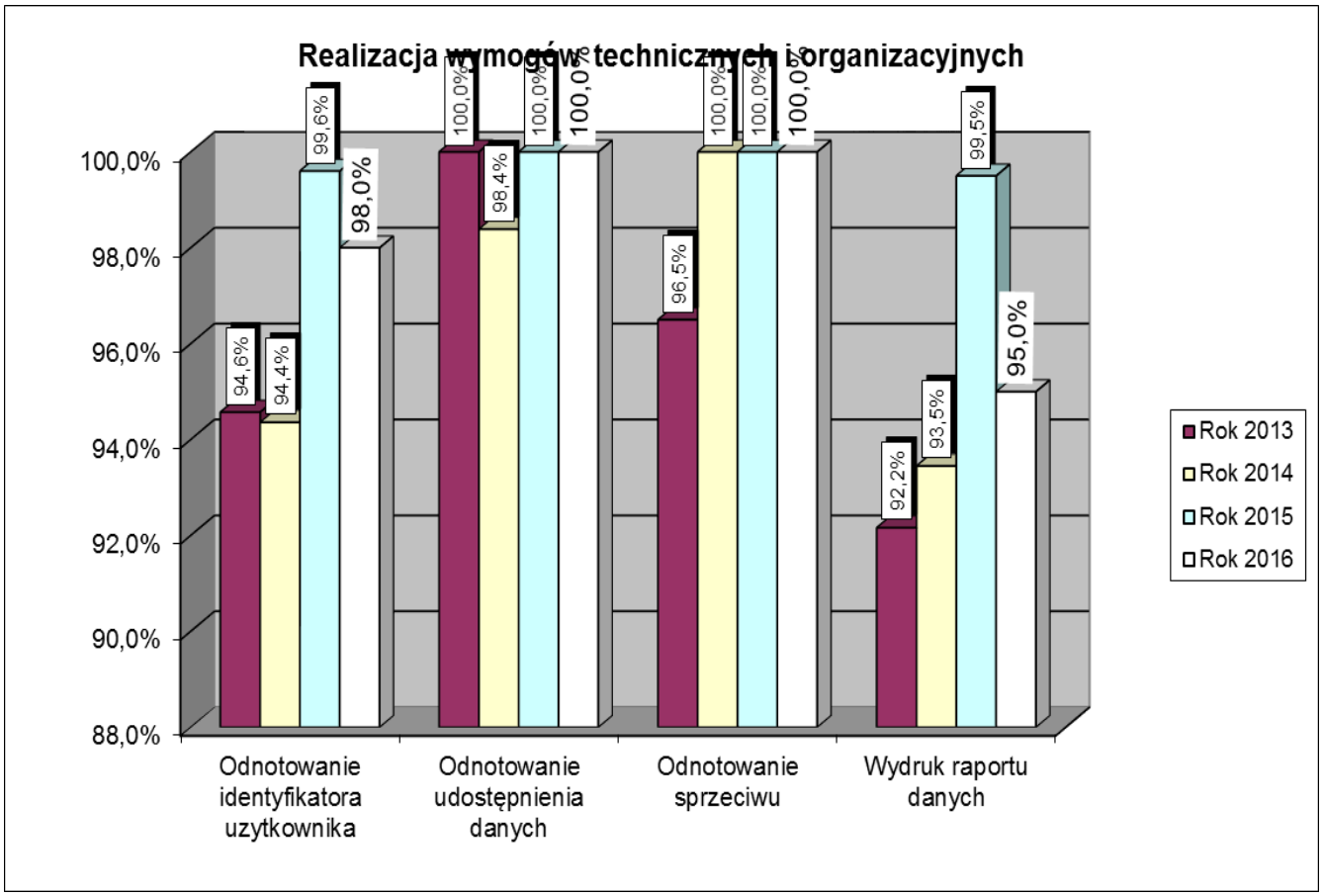
Systemy te wykorzystywały różnorodne rozwiązania technologiczne, od najprostszych, gdzie zbiory danych osobowych przetwarzane były z wykorzystaniem powszechnie dostępnych aplikacji biurowych (edytorów tekstu, arkuszy kalkulacyjnych), po najbardziej rozbudowane oparte o zaawansowane mechanizmy bazodanowe.

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 wa-

runkami określonymi w §7 ust. 4 rozporządzenia, poszczególne warunki uznawano dla systemu objętego kontrolą jako spełnione. Stopień realizacji wymogów o charakterze techniczno-organizacyjnym dla systemów informatycznych objętych kontrolą w roku 2016 w porównaniu do lat 2013-2015 przedstawiono na poniższych wykresach.



Wykres 4. ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2013 – 2016 – część I.***

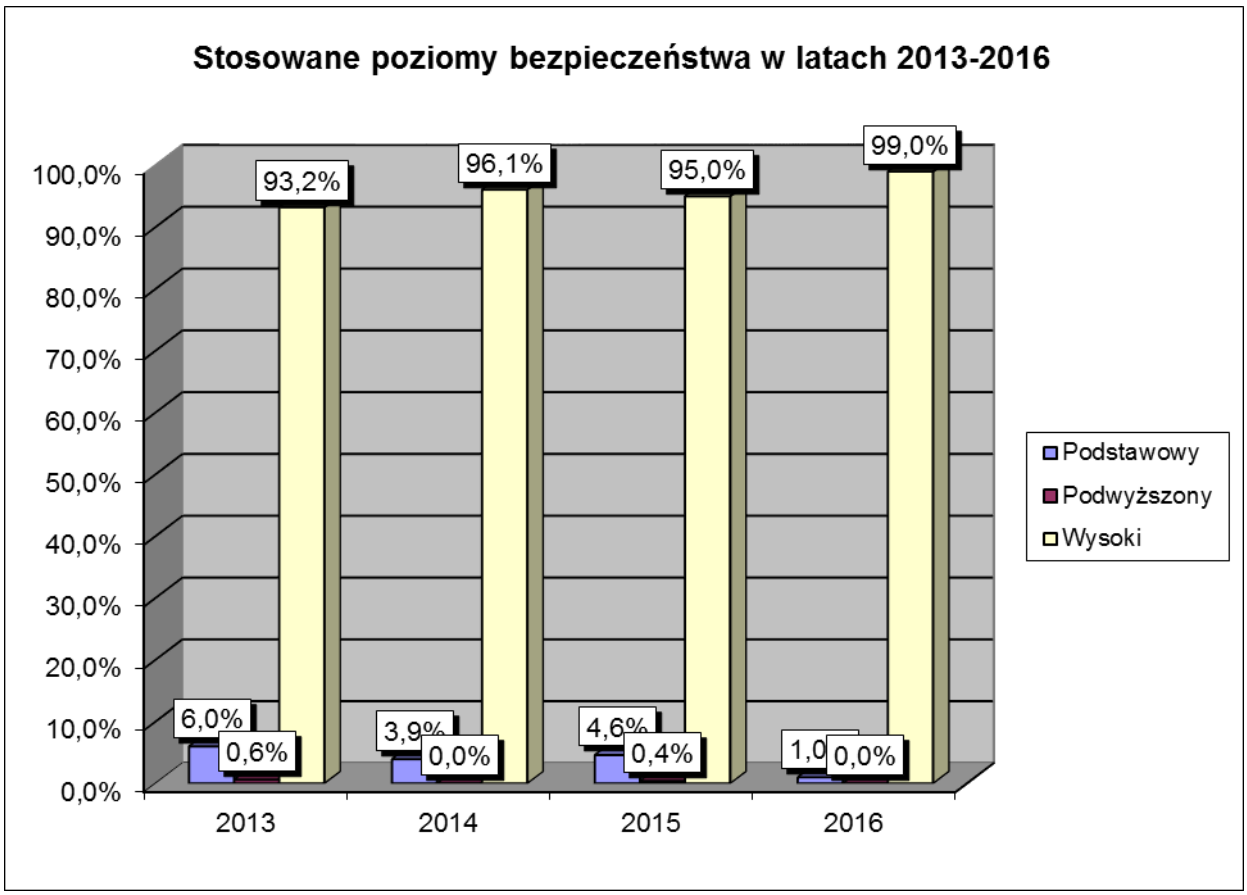


Wykres 5. ***Stopień realizacji wymogów technicznych i organizacyjnych w latach 2013 – 2016 – część II.***

Jak wynika z wykresu nr 4, liczba systemów informatycznych objętych kontrolą w roku 2016 była znacznie wyższa niż w latach poprzednich. Fakt ten wynikał z tego, że w ramach sprawdzeń realizowanych przez administratorów bezpieczeństwa informacji na wniosek GIODO badane były instytucje finansowe, które do przetwarzania danych osobowych wykorzystują dużą ilość systemów informatycznych.

Zapewnienie funkcjonalności związanych z odnotowywaniem, przez objęte w 2016 roku oceną systemy informatyczne, informacji o dacie iidentyfikatorze użytkownika wprowadzającego dane jak również możliwość sporządzenia raportów z ww. odnotowaniami kształtuje się na poziomie zbliżonym do lat poprzednich.

3.4.3. Ocena poziomu bezpieczeństwa



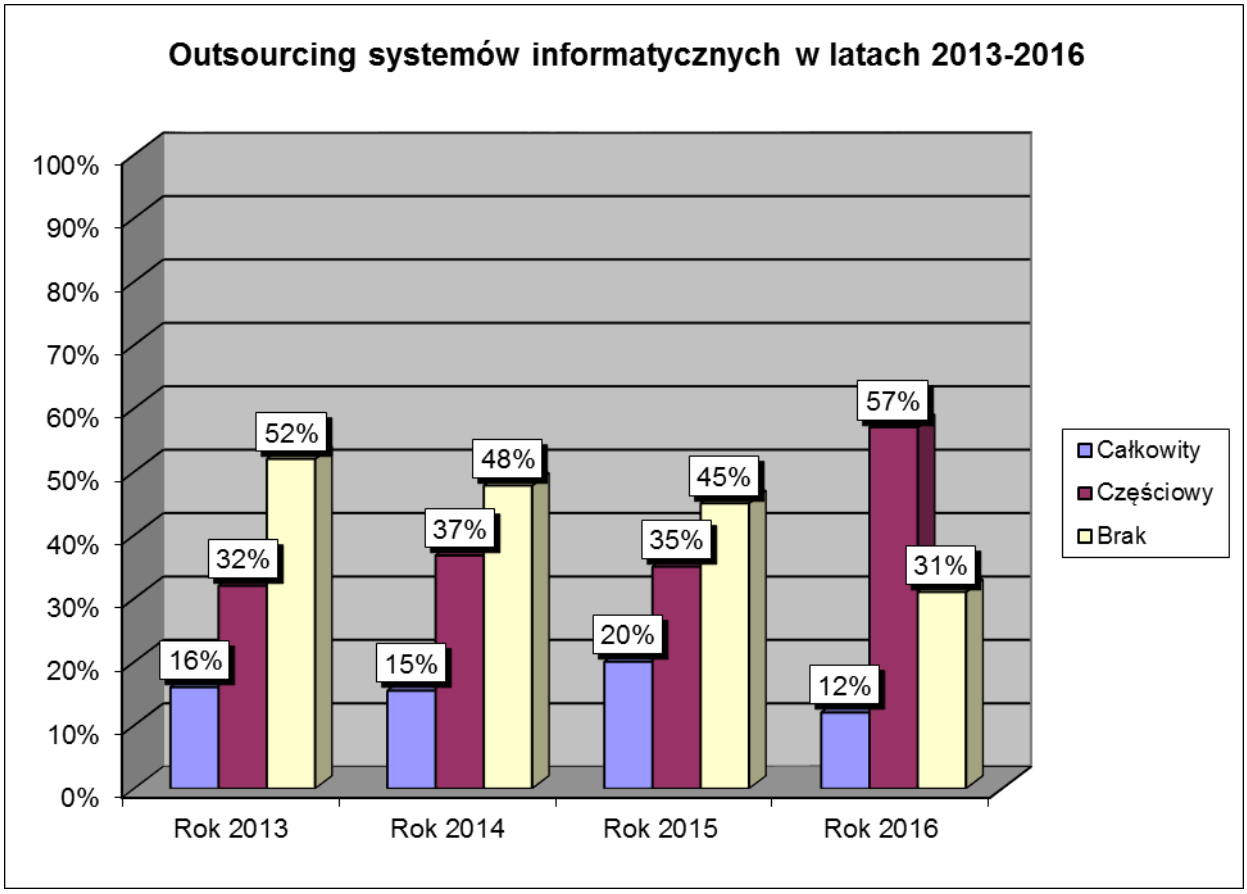
Wykres 6. ***Podział na poziomy bezpieczeństwa zastosowane dla systemów informatycznych poddanych ocenie w latach 2013-2016.***

Jak wynika z powyższego wykresu, niemal wszystkie skontrolowane w 2016 r. podmioty (99%) zastosowały wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych.

3.4.4. Outsourcing i kolokacja danych.

Jak wynika z przeprowadzonych w 2016 r. kontroli, większość podmiotów wykorzystywało do przetwarzania danych osobowych systemy informatyczne, nad którymi sprawowały częściową 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 2016 r. stosowany był w odniesieniu do

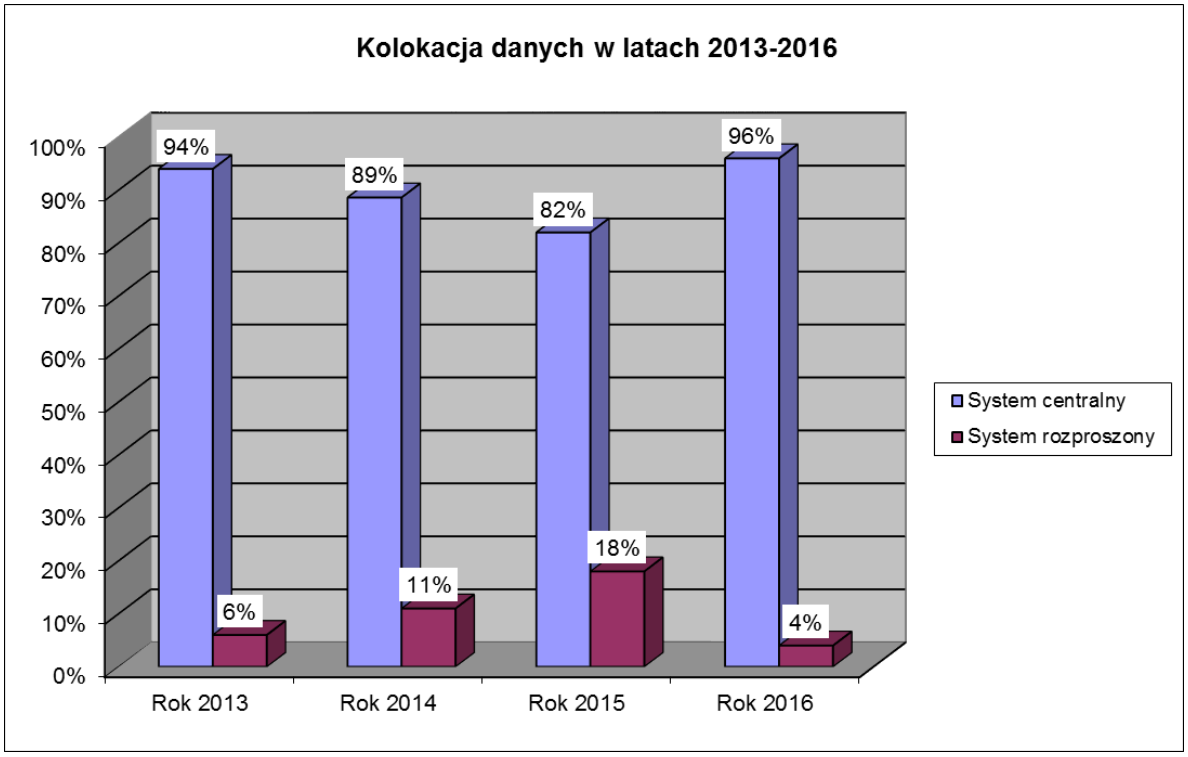
około 12 % systemów informatycznych. Jest to liczba nieco mniejsza niż w latach ubiegłych. W 2016 r. zauważono również niewielki spadek liczby tych systemów informatycznych, których obsługą techniczną i administracją zajmowali się wyłącznie pracownicy administratora danych (31% systemów informatycznych).



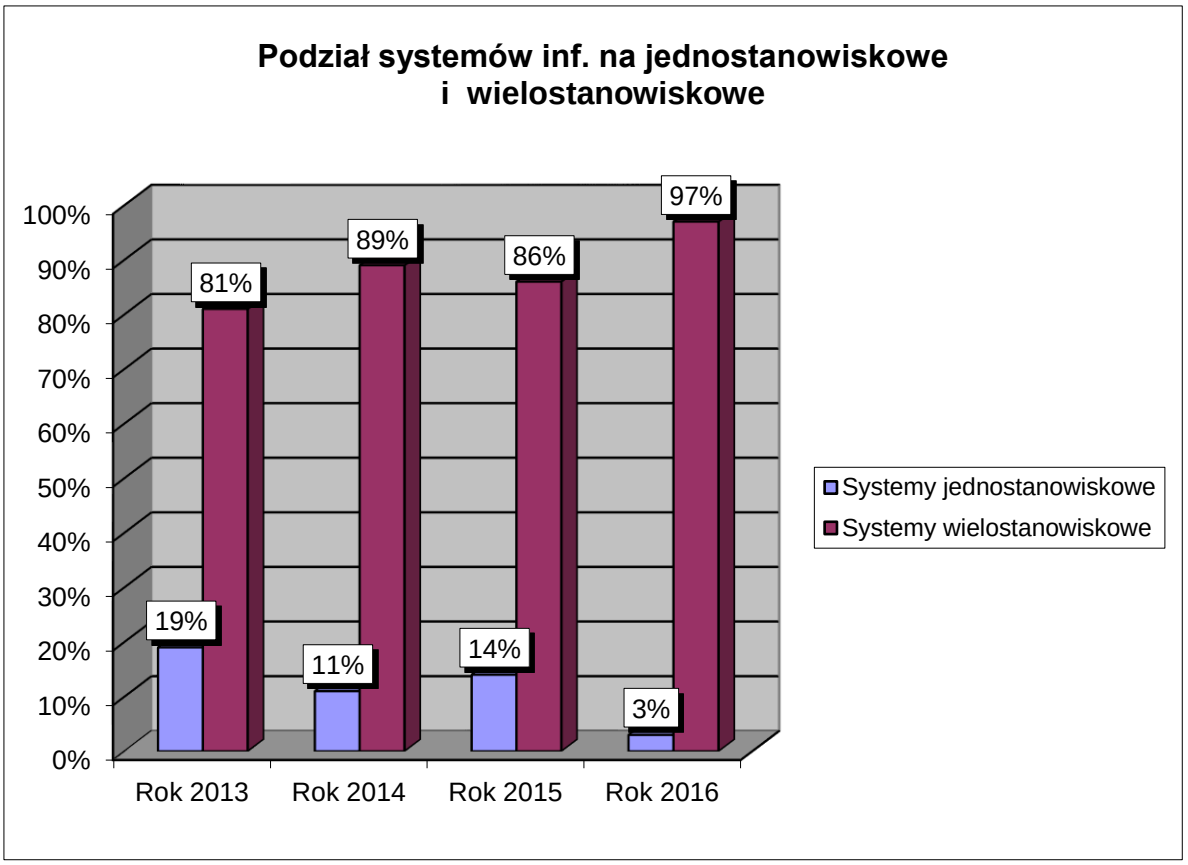
Wykres 7. ***Ilościowy udział outsourcingu systemów informatycznych w latach 2013 – 2016.***

3.4.5. Systemy centralne i rozproszone

W większości skontrolowanych podmiotów dane osobowe zapisywane były w jednym, centralnym miejscu, np. na serwerze/serwerach znajdujących się w jednej lokalizacji, zazwyczaj w siedzibie kontrolowanego podmiotu. Zauważyć jednak należy, że w stosunku do lat poprzednich zmniejszyła się liczba podmiotów wykorzystujących do przetwarzania danych osobowych systemy rozproszone. Na poniższym wykresie przedstawiono stopień stosowania przez kontrolowane podmioty rozwiązań technicznych opartych o systemy centralne i rozproszone.



Wykres 8. ***Procentowy udział centralnego przetwarzania danych w systemach informatycznych poddanych ocenie w latach 2013 - 2016.***



Wykres 9. ***Procentowy udział systemów informatycznych jedno i wielostanowiskowych poddanych ocenie w latach 2013 - 2016.***

3.4.6. Wybrane zagadnienia dotyczące kontroli niesektorowych

Jedną z ciekawostek, jaką zaobserwowano podczas czynności kontrolnych w 2016 r. był mechanizm o nazwie screen scraping (zdrapywanie ekranu). Polega on na automatycznym zasysaniu danych klienta z kont w innych instytucjach finansowych, np. w celu zbadania zdolności kredytowej. Operację przeprowadza dedykowany do tego celu program komputerowy, który po pobraniu danych sprowadza je do jednolitego formatu. Wskazany program rozpoczyna pobieranie danych po podaniu przez klienta loginów i haseł do swoich kont bankowych. Od 2014 r. stosowanie tej metody w Polsce jest zakazane. Komisja Nadzoru Finansowego stoi bowiem na stanowisku, że zgodnie z umową rachunku, klient nie może nikomu, za wyjątkiem własnego banku, przekazywać danych do logowania.

Interesującym rozwiązaniem był również system informatyczny, służący do diagnozy pacjenta w ramach opieki telemedycznej na odległość. System składał się ze stanowiska klienckiego, funkcjonującego na komputerze typu PC oraz ze stacji serwerowej. Komputer PC posiadał wbudowaną kamerę, mikrofon i głośniki, możliwe jest też podłączenie zewnętrznych słuchawek z mikrofonem. Urządzenie do poprawnego działania, oprócz zasilania z sieci elektrycznej wymaga przewodowego lub bezprzewodowego dostępu do sieci Internet (warunek konieczny do połączenia stacji klienta ze stacją serwerową na odległość). Stacja kliencka służyła do wprowadzania ręcznie wyników w zakresie parametrów fizjologicznych pacjentów, takich jak: ciśnienie krwi, poziom cukru we krwi, tętno serca, temperatura ciała i waga. Na stacji klienckiej nie były zachowywane informacje i po wybraniu przycisku „wyślij" przesyłane były do stacji serwerowej. Dostęp dla pacjentów po stronie stacji klienckiej realizowany jest po wprowadzeniu danych identyfikacyjnych, tj. numeru PESEL danego pacjenta. Stacja kliencka umożliwia przesyłanie informacji w formie audio-wideo oraz w trybie tekstowym. Ponadto stacja kliencka umożliwia podłączenie przez port USB urządzeń pomiarowych, takich jak EKG, ciśnieniomierz, glukometr.

W opisanych wyżej przypadkach trwa analiza zgromadzonego w toku kontroli materiału dowodowego niezbędna dla oceny, czy doszło do naruszenia przepisów o ochronie danych osobowych, czy też dane są przetwarzanie zgodnie z obowiązującym prawem. Konieczne może także okazać się przeprowadzenie czynności kontrolnych w podmiotach współpracujących z podmiotami stosującymi ww. rozwiązania, np. w podmiocie oferującym system informatyczny umożliwiającym pobieranie danych z wykorzystaniem mechanizmu „screen scraping". Takie kontrole zostaną przeprowadzone w 2017 r.

4. Egzekucja administracyjna – zapewnienie wykonania decyzji

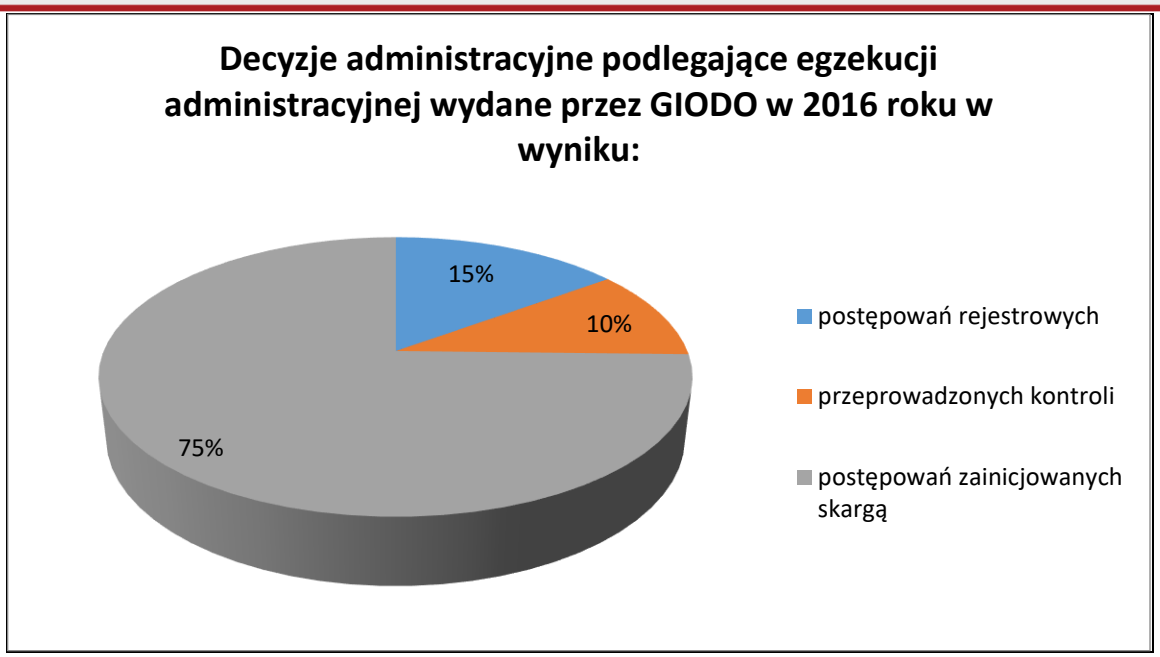
W celu zapewnienia wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych, Generalny Inspektor – na podstawie art. 12 pkt 3 ustawy o ochronie danych osobowych - uprawniony jest do stosowania środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. z 2016 r., poz. 599 z późn. zm.).

Egzekucji administracyjnej podlegają wszystkie decyzje administracyjne Generalnego Inspektora nakładające na strony obowiązek (nakaz) do wykonania, które są ostateczne oraz te, którym nadano rygor natychmiastowej wykonalności.

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

W 2016 r. Generalny Inspektor Ochrony Danych Osobowych wydał 67 decyzji administracyjnych zawierających nałożony na strony nakaz (obowiązek) do wykonania i podlegających egzekucji administracyjnej.

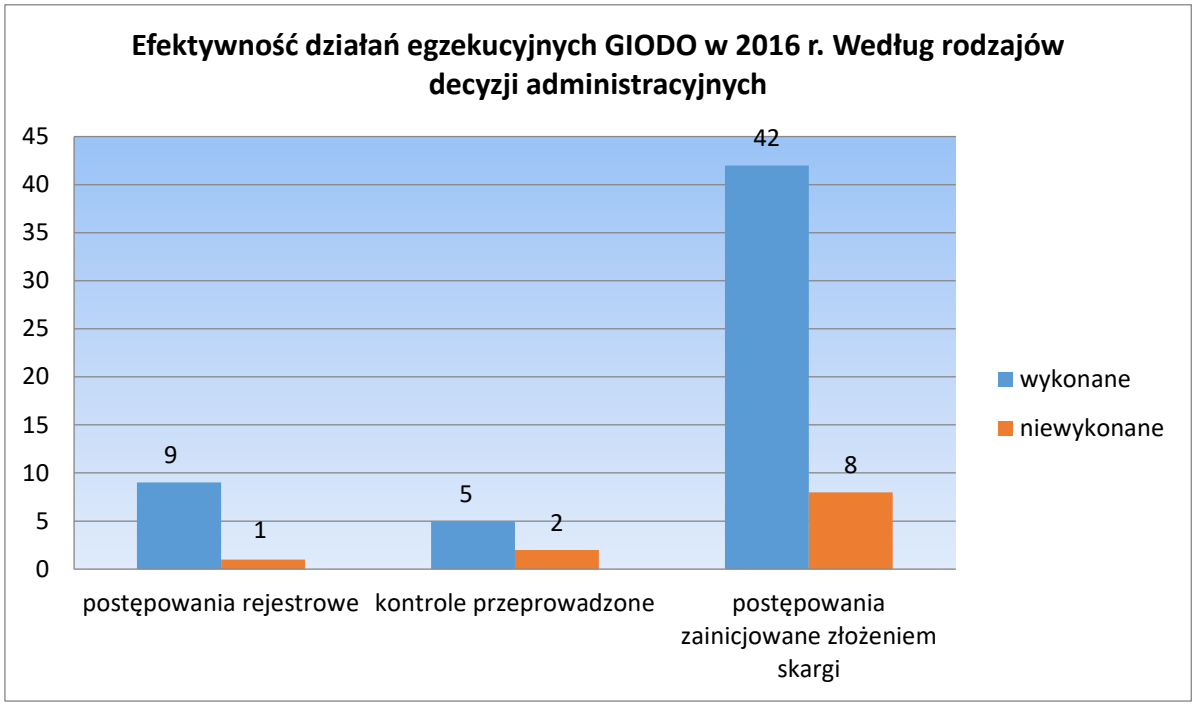
Spośród decyzji wydanych w 2016 r. 10 dotyczyło postępowań rejestrowych, 7 zostało wydanych w związku z przeprowadzonymi inspekcjami (kontrolami), 50 wydano na skutek postępowania zainicjowanego skargą.



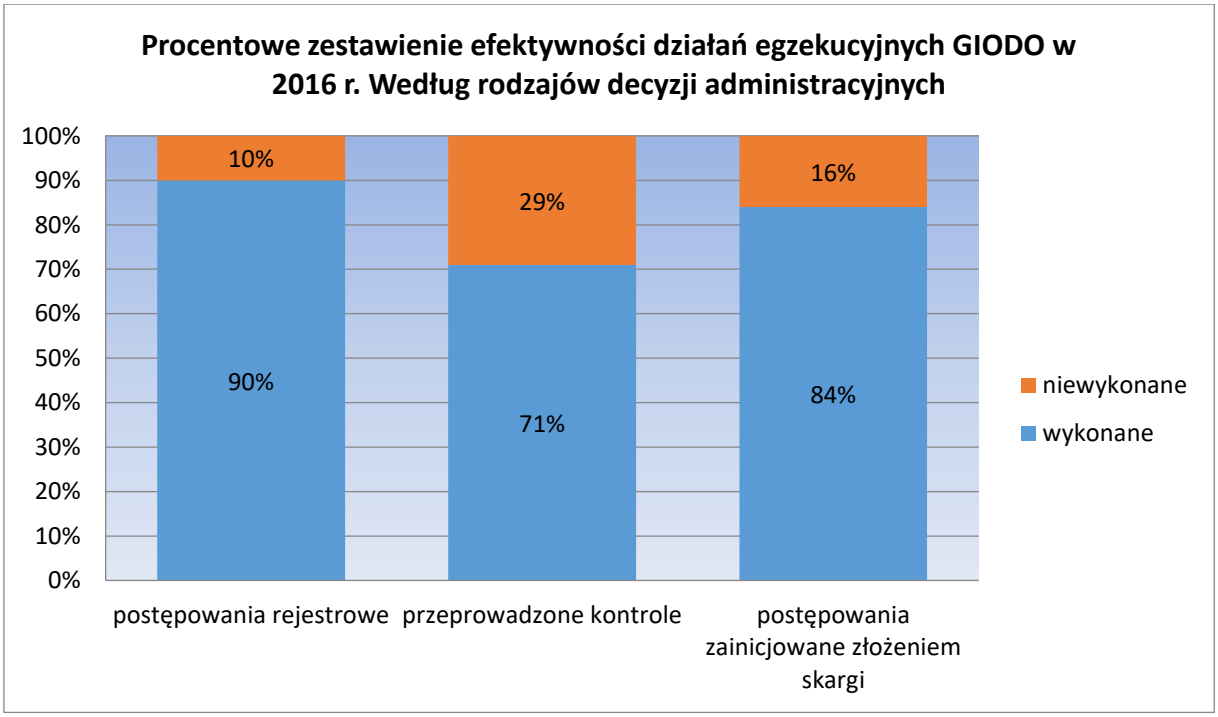
Wykres 10. ***Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2016 r.***

Efektywność prowadzonych przez Generalnego Inspektora działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków w 2016 r. przedstawia się następująco: spośród 67 decyzji administracyjnych **wykonanych zostało przez zobowiązanych 56 decyzji**, 11 decyzji na koniec 2016 r. pozostało niewykonanych. Decyzje te objęte są działaniami egzekucyjnymi w 2017 r. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań Generalnego Inspektora oraz przeprowadzonych kontroli sprawdzających. W 5 przypadkach wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia zobowiązani w 4 przypadkach wykonali w całości decyzję administracyjną Generalnego Inspektora.

Spośród decyzji wydanych w 2016 r. i wykonanych przez zobowiązanych w 2016 r. wskutek działań Generalnego Inspektora **9** dotyczyło postępowań rejestrowych, **5** zostało wydanych w związku z przeprowadzonymi kontrolami, **42** wydano na skutek postępowania zainicjowanego skargą. Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w 2016 r. wynosi **84%.** W odniesieniu do postępowań rejestrowych efektywność egzekucji wynosi **90%**, wobec decyzji wydanych w związku z przeprowadzonymi kontrolami - **71%**, natomiast w stosunku do decyzji wydanych na skutek postępowań zainicjowanych skargą - **84%**.



Wykres 11. ***Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2016 r.***

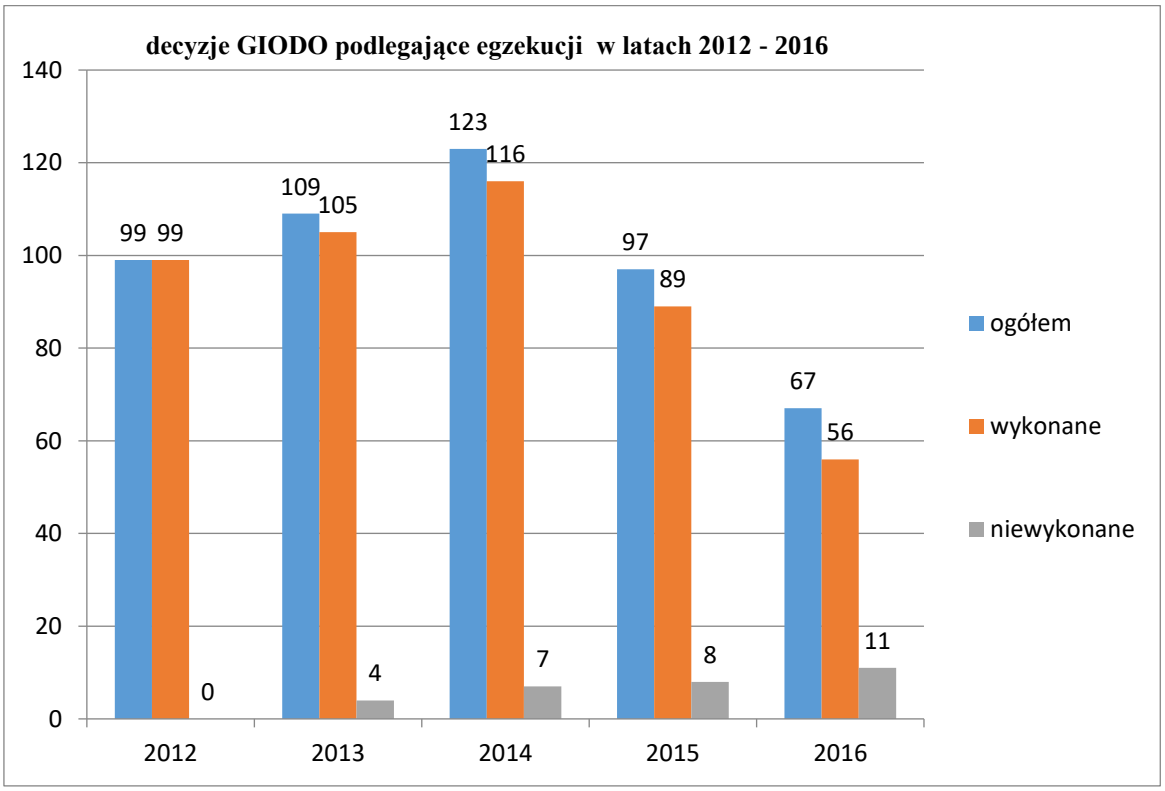


Wykres 12. ***Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO w 2016 r.***

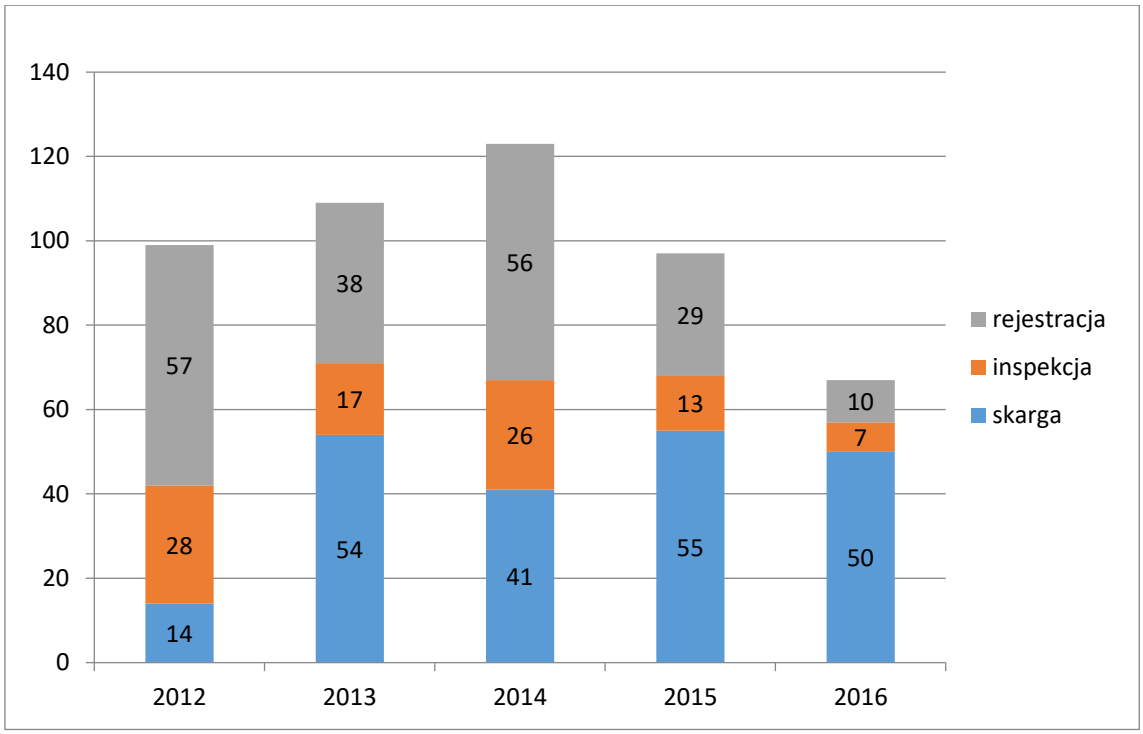
Można zaobserwować kontynuację trendu w odniesieniu do decyzji administracyjnych wydawanych przez GIODO a podlegających egzekucji administracyjnej. W 2013 r. decyzji było 109. W 2014 r. do egzekucji przekazano 123 decyzje, co stanowi wzrost o 13% w stosunku do roku poprzedniego. Natomiast w 2015 r. wpłynęło 97 decyzji administracyjnych, co stanowi spadek o 21% w stosunku do roku poprzedniego. W 2016 r. odnotowano wpływ 67 decyzji administracyjnych, co stanowi spadek o 31% w stosunku do roku poprzedzającego.

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora wydanych w latach 2012-2016 przedstawia się następująco: spośród decyzji GIODO objętych egzekucją administracyjną w 2012 r - efektywność wynosi **100%**, natomiast w zakresie decyzji GIODO objętych egzekucją administracyjną w 2013 r. efektywność wynosi **96%.** W odniesieniu do postępowań egzekucyjnych prowadzonych w 2014 r. efektywność egzekucji wynosi **94%**, natomiast w odniesieniu do postępowań egzekucyjnych prowadzonych w 2015 r. efektywność egzekucji wynosi **92%.**

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do decyzji administracyjnych Generalnego Inspektora wydanych w 2016 r. wynosi **84%.** Niższy wskaźnik efektywności w odniesieniu do 2016 r. wynika z faktu, iż wobec tych decyzji działania egzekucyjne zostały rozpoczęte niejednokrotnie pod koniec roku, zobowiązani sukcesywnie wykonują nakazy zawarte w decyzjach i są w trakcie składania informacji o wykonaniu decyzji do Generalnego Inspektora.



*Wykres 13. Z**estawienie decyzji GIODO podlegających egzekucji administracyjnej i efektywność podejmowanych działań egzekucyjnych w latach 2012 – 2016.***



*Wykres 14. Z**estawienie decyzji GIODO podlegających egzekucji administracyjnej ze względu na źródło pochodzenia nakazu w latach 2012 – 2016.***

5. Opiniowanie aktów prawnych i rozporządzeń dotyczących ochrony danych osobowych

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 2016 r. realizacja tych zadań przez Generalnego Inspektora Ochrony Danych Osobowych w dużej mierze była powiązana z informowaniem innych organów o wymogach, jakie będzie na nie oraz na innych administratorów danych nakładać ogólne rozporządzenie o ochronie danych osobowych (np. zasady privacy by design, privacy by default, privacy impact assessment). GIODO w przygotowywanych opiniach wskazywał przy tym na konieczność uwzględniania postanowień ogólnego rozporządzenia w projektowanych aktach prawnych. Tendencja ta staje się coraz bardziej widoczna, jako że przepisy rozporządzenia będą w sposób bezpośredni stosowane w polskim porządku prawnym od 25 maja 2018 r.

Generalny Inspektor Ochrony Danych Osobowych z zadowoleniem odnotowuje, iż coraz więcej podmiotów, w tym projektodawców, uświadamia sobie wyzwania związane z koniecznością dostosowania krajowych przepisów do wspomnianych wyżej regulacji unijnych i współpracuje w tym zakresie z organem do spraw ochrony danych. Generalny Inspektor stara się w miarę możliwości wspomagać projektodawców w wypracowaniu rozwiązań, które będą zgodne z zasadami ochrony danych osobowych, a jednocześnie realizować będą cele projektodawcy. Argumenty przedstawiane przez GIODO mają na celu wsparcie projektodawców w wypracowaniu takich przepisów, które w odpowiedni sposób równoważyć będą interesy i potrzeby wszystkich zainteresowanych stron, w tym osób, których dane dotyczą, tj. podmiotów danych, ale i adresatów zmienianych czy uchwalanych norm prawa, a zatem administratorów danych, którymi są podmioty sektora publicznego czy przedsiębiorcy.

Wielokrotnie wprowadzanie nowych rozwiązań związanych z przetwarzaniem danych osobowych w systemach teleinformatycznych motywowane jest przez projektodawców chęcią wprowadzania ułatwień dla obywateli. Pamiętać jednak należy - i w tym zakresie GIODO przestrzega projektodawców przed tworzeniem przepisów niejasnych, niespójnych czy niewystarczających - iż musi się ono odbywać z poszanowaniem zasad ochrony danych osobowych, bowiem tylko wówczas planowane rozwiązania będą mogły funkcjonować w sposób zgodny z prawem. Jasne i przejrzyste rozpisanie zasad przetwarzania danych osobowych jest niezbędne, aby osoby, których dane dotyczą, miały świadomość, kto, w jakim zakresie, w jaki sposób, w jakich celach oraz przez jaki okres przetwarza dotyczące ich informacje.

W roku 2016 w Biurze GIODO przeanalizowano 722 projekty aktów prawnych (czyli o 19 projektów więcej niż w roku poprzednim).

Należy zwrócić uwagę, że 52 projekty były analizowane przez Generalnego Inspektora z urzędu, gdyż nie zostały przekazane przez projektodawcę do uzgodnienia bądź konsultacji.

W podziale na poszczególne miesiące 2016 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła następująca liczba projektów aktów prawnych: styczeń - 29, luty - 36, marzec - 37, kwiecień - 53, maj - 63, czerwiec - 79, lipiec - 86, sierpień - 66, wrzesień - 57, październik - 46, listopad - 80, grudzień – 90.

W niniejszej informacji wskazane zostały najbardziej istotne projekty - i związane z nimi prace legislacyjne - w odniesieniu do których opinie zgłosił Generalny Inspektor Ochrony Danych Osobowych w analizowanym roku sprawozdawczym.

WĄTPLIWA ZMIANA KONCEPCJI ADMINISTRATORA DANYCH

W 2016 r. kontynuowano prace legislacyjne nad projektem ustawy o pomocy państwa w wychowywaniu dzieci (druk sejmowy nr 216)[77], Zasadnicze wątpliwości organu do spraw ochrony danych osobowych wzbudziła – zawarta w art. 38 projektu – propozycja zmiany ustawy o ochronie danych osobowych, która nie była konsultowana z Generalnym Inspektorem Ochrony Danych Osobowych.

Zmiana ta wprowadzona została do projektu podczas obrad Stałego Komitetu Rady Ministrów, co uniemożliwiło organowi do spraw ochrony danych osobowych wyrażenie opinii w tym zakresie. Taki sposób procedowania projektu jest nie do zaakceptowania przez Generalnego Inspektora Ochrony Danych Osobowych, tym bardziej że projektowane regulacje zmieniające ustawę o ochronie danych osobowych odnosić się będą do praw podstawowych jednostek, a ostateczny kształt przepisów w sposób bezpośredni dotyczył będzie podstawowych zasad ochrony danych osobowych. Co więcej – wprowadzenie zmian do przepisów ustawy o ochronie danych osobowych, czyli aktu prawnego o charakterze ogólnym, niejako „przy okazji" procedowania regulacji dotyczącej świadczenia wychowawczego, uznać należało za niebezpieczny precedens, który nie powinien był mieć miejsca.

Projektowane zmiany ustawy o ochronie danych osobowych stały w sprzeczności z przepisami dyrektywy 95/46/WE[78], której ustawa o ochronie danych osobowych stanowi implementację. Koncepcje przewidziane przez Projektodawcę były całkowicie niedopuszczalne z punktu widzenia przepisów prawa Unii Europejskiej, które to prawo nie przewiduje analogicznych rozwiązań. Wobec powyższego przyjęcie proponowanych unormowań skutkować mogło zarzutem błędnej implementacji dyrektywy 95/46/WE Parlamentu Europej-

[77] DOLiS-033-32/16.

[78] Dyrektywa 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.

skiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Dotychczasowy – wypracowany na podstawie przepisów prawa Unii Europejskiej – model ochrony danych osobowych opierał się na konstrukcji administratora danych, czyli najważniejszego podmiotu w procesie przetwarzania danych, decydującego o celach i środkach przetwarzania danych osobowych (art. 7 pkt 4 ustawy o ochronie danych osobowych). Ten administrator danych, zarówno ze względu na ciążące na nim rozliczne obowiązki wynikające z przepisów o ochronie danych osobowych, jak i posiadane przez niego uprawnienia w procesie przetwarzania danych, musi być jednoznacznie zidentyfikowany. **Tymczasem projekt, wprowadzając koncepcję administratora danych, którego można by nazwać „zbiorowym" albo „łącznym", albo „wspólnym", odstępował od dotychczasowego modelu ochrony danych osobowych.**

GIODO zauważył przy tym, że zmiany w polskich przepisach dotyczących ochrony danych osobowych są nieuniknione ze względu na przyjęcie ogólnego rozporządzenia o ochronie danych, które po dwuletnim okresie *vacatio legis* będzie obowiązywać we wszystkich państwach członkowskich Unii Europejskiej. Zobliguje to ustawodawcę polskiego do przeprowadzenia przeglądu całego krajowego ustawodawstwa pod kątem jego zgodności z przepisami rozporządzenia UE. Tymczasem proponowane w projekcie zmiany ustawy o ochronie danych osobowych stały w sprzeczności z rozwiązaniami już przyjętymi w projekcie ogólnego rozporządzenia, a więc aktu prawnego, który po zakończeniu dotyczącej go procedury legislacyjnej będzie obowiązywał w Rzeczypospolitej Polskiej w sposób bezpośredni (wykluczone zatem będzie kreowanie jakichkolwiek odmiennych rozwiązań przez ustawodawcę krajowego).

Z przytoczonych wyżej przyczyn Generalny Inspektor Ochrony Danych Osobowych wniósł o wykreślenie z projektu ustawy o pomocy państwa w wychowywaniu dzieci art. 38. Postulaty te nie zostały jednak uwzględnione.

REJESTR INFORMACJI O RACHUNKACH BANKOWYCH

Wśród opiniowanych przez GIODO projektów aktów prawnych znalazł się ponadto projekt ustawy o Centralnej Bazie Rachunków[79]. **Projekt zakładał zgromadzenie w jednym miejscu informacji o niemal wszystkich formach przechowywania środków finansowych** – to jest informacji o rachunkach bankowych. Rejestr miał być aktualizowany w ciągu 24 godzin od utworzenia konta lub jego modyfikacji. Centralna Baza Rachunków miała gromadzić informacje o osobach fizycznych oraz prawnych i jednostkach nieposiadających osobowości prawnej.

W swojej opinii dotyczącej tego projektu Generalny Inspektor Ochrony Danych Osobowych wskazał, iż organowi do spraw ochrony danych osobowych nie jest znany cel, dla którego Minister Finansów miałby stworzyć unikalny na skalę krajową zbiór danych o rachunkach zawierający dane osobowe większości obywateli, jak również innych osób posiadających szeroko rozumiane rachunki produktów finansowych na terenie Polski. Nie jest również jasne, jakie cele przy pomocy tak utworzonej bazy danych miałby realizować Minister Finan-

[79] DOLiS-033-633/16

sów, który nie jest organem prowadzącym postępowania w sprawach z zakresu lokalizowania składników majątkowych pochodzących z przestępstwa.

Zgodnie z projektem, nowe przepisy miały określać postępowanie przy przetwarzaniu informacji o rachunkach w celu ustalenia miejsca przechowywania wartości majątkowych mogących mieć związek z przestępstwem lub podlegających egzekucji sądowej lub administracyjnej. Ani z treści projektowanej ustawy, ani uzasadnienia nie wynikało, kto i jak będzie tę przesłankę oceniał. Przy bardzo szerokiej jej interpretacji, właściwie każda wątpliwość w tym zakresie może stanowić podstawę pozyskiwania określonych informacji o rachunkach, w tym danych osobowych. Na instytucje zobowiązane nałożony miałby zostać obowiązek przekazywania do Centralnej Bazy Rachunków informacji o rachunkach - w przypadku otwarcia rachunku, zmiany przekazanych informacji o rachunku i jego zamknięcia. Sposób funkcjonowania bazy nie zawiera opisu systemu, w jaki tak duża ilość danych osobowych i innych informacji o rachunkach będzie podlegała przekazywaniu między instytucjami zobowiązanymi do przekazywania tychże danych, Ministrem Finansów (administratorem danych zgromadzonych w Centralnej Bazie Rachunków i organem właściwym), jak również 13 podmiotami wymienionym w projekcie, którym te dane mają być udostępniane. Zarówno mechanizm polegający na udostępnianiu informacji o rachunku w czasie rzeczywistym, w postaci elektronicznej, jak również przekazanie kopii informacji o rachunkach Centralnej Bazy Rachunków lub ich podzbiorów, w terminie i formie ustalonych w porozumieniu z organem właściwym, budzi sprzeciw Generalnego Inspektora Ochrony Danych Osobowych. Brak jest bowiem mechanizmu kontroli dostępu do rejestrów, co stwarza ryzyko nadużyć polegających na nieuzasadnionym udostępnianiu danych.

W zakresie, w jakim projektodawca przyznaje podmiotom uprawnionym prawo do przekazywania udostępnionych informacji o rachunkach innym podmiotom krajowym oraz poza granicę kraju, jeśli jest to konieczne do zapobiegania przestępstwom, do prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo do wykonywania kar, jeśli przepisy odrębne tak stanowią – była w ocenie organu do spraw ochrony danych osobowych upoważnieniem blankietowym. Zdaniem Generalnego Inspektora Ochrony Danych Osobowych, w projekcie ustawy o Centralnej Bazie Rachunków powinno być wymienione dla jakich celów, w jakim zakresie, jak i na podstawie jakich przepisów prawnych dane te będą przekazywane i kto będzie dokonywał oceny konieczności/zasadności takiego transferu.

Organ do spraw ochrony danych osobowych wyraził również wątpliwość co do braku ustawowego uregulowania (lub stosownej informacji podanej w uzasadnieniu projektowanej ustawy) dotyczącego sposobu wykorzystania danych udostępnionych podmiotom uprawnionym, w przypadku, gdy dane te okazały się nieprzydatne z punktu widzenia prowadzonych postępowań.

Niezgodne z zasadami ochrony danych osobowych było również tworzenie kopii rejestrów dla innego organu, a także przekazywanie zbioru spełniającego wszystkie kryteria uznania go jako big data w formie porozumienia Ministra Finansów z Generalnym Inspektorem Informacji Finansowej. Wskazać przy tym należało, iż postanowienia projektowanej ustawy nie zawierały informacji o celu, zakresie, zasadach przetwarzania (w tym retencji), kopii in-

formacji o rachunkach Centralnej Bazy Rachunków przekazywanych Generalnemu Inspektorowi Informacji Finansowej.

Uzupełnienia wymagała również treść art. 11 projektu ustawy o Centralnej Bazie Rachunków. Chodziło mianowicie o brak mechanizmu weryfikacyjnego pozyskanych danych po upływie 10-letniego terminu ich retencji. Projektodawca nie wyjaśnił, w jaki sposób zamierzał dokonywać klasyfikacji tychże danych ani ich usuwania, gdy zyskają status zbędnych. Analogiczna uwaga dotyczyła treści art. 20 ust. 2 projektowanej ustawy.

GIODO za konieczne uznał również wyjaśnienie powodów, dla których projektodawca wyłączył stosowanie przepisów art. 24, art. 32 ust. 1 pkt 3 i 5, art. 47 i art. 48 ustawy o ochronie danych osobowych (art. 21 projektowanej ustawy), gdyż brak było w tym zakresie odniesienia w uzasadnieniu projektu. Należało bowiem mieć na względzie sytuację, w której w przypadku uchwalenia projektowanej ustawy w proponowanym brzmieniu, do organu do spraw ochrony danych osobowych będą wpływały skargi osób fizycznych na niezgodne z prawem przetwarzanie ich danych osobowych, w tym również przekazanie ich danych osobowych do państwa trzeciego bez podstawy prawnej.

Wyjaśnienia wymagał również zapis art. 18 projektowanej ustawy, w którym jest mowa o wyłączeniu przepisów ograniczających udostępnienie danych objętych tajemnicą, z wyjątkiem informacji niejawnych – w zakresie, w jakim jest w nim mowa o „tajemnicy", bez określenia, o jaką tajemnicę projektodawcy chodzi.

W dacie sporządzania niniejszego sprawozdania projekt ustawy o Centralnej Bazie Rachunków nadal znajdował się na etapie opiniowania, a projektodawca nie odniósł się do przedstawionych uwag.

CO WOLNO SŁUŻBOM?

Dwukrotnie w ubiegłym roku, w toku prac rządowych i parlamentarnych, Generalny Inspektor wnosił uwagi do projektu **ustawy o działaniach antyterrorystycznych**[80]. Odnosząc się do całości projektu, Generalny Inspektor ponownie zwrócił uwagę na kwestię braku zapewnienia zewnętrznej kontroli przetwarzania danych przez Agencję Bezpieczeństwa Wewnętrznego sprawowanej przez niezależny, autonomiczny organ. Zapewnienie istnienia tego rodzaju kontroli jest obowiązkiem ustawodawcy, zwłaszcza w świetle stanowiska wyrażonego w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 roku (sygn. akt K 23/11). W opinii organu do spraw ochrony danych osobowych, prowadzone w Sejmie Rzeczypospolitej Polskiej prace dotyczące projektu były najbardziej prawidłowym momentem dla podjęcia działań legislacyjnych zmierzających do powołania podmiotu zapewniającego niezależną, zewnętrzną kontrolę przetwarzania danych przez wszystkie służby specjalne (ewentualnie nadania kompetencji do sprawowania takiej kontroli jakiemuś podmiotowi już istniejącemu), tym bardziej że Generalnemu Inspektorowi Ochrony Danych Osobowych nic nie jest wiadome na temat kontynuowania, podjętych przez Ministerstwo Spraw Wewnętrznych w 2013 roku, prac dotyczących projektu *ustawy o Komisji Kontroli Służb Specjalnych*[81] czy też projektu ustawy regulującej funkcjonowanie Agencji Bezpieczeństwa Wewnętrznego, które toczyły się

[80] DOLiS-033-133/16.
[81] https://legislacja.rcl.gov.pl/projekt/181401/katalog/181409#181409. DOLiS-033-442/13/71667

w 2014 r.[82] Z aprobatą GIODO przyjął natomiast fakt zamieszczenia w przepisach ustawowych unormowań określających katalog osób związanych z działaniami terrorystycznymi. Uwadze Generalnego Inspektora nie umknęło jednocześnie, iż – w myśl art. 93 ust. 1 i 2 Konstytucji Rzeczypospolitej Polskiej – akt prawny o charakterze wewnętrznym, jakim jest zarządzenie, nie może stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów. Tym samym – w świetle uwarunkowań konstytucyjnych – za wysoce kontrowersyjną uznał konstrukcję prawną, zgodnie z którą podstawowe regulacje dotyczące wykazu (zakres informacji w nim gromadzonych, tryb udostępniania z niego informacji etc.) znaleźć się miały w zarządzeniu (niejawnym) Szefa Agencji Bezpieczeństwa Wewnętrznego. GIODO wskazał, że z jednej strony trudno było racjonalnie przyjąć, że fakt umieszczenia informacji o danej osobie w wykazie nie będzie skutkować podejmowaniem wobec tej osoby określonych decyzji przez polskie organy władzy publicznej, z drugiej – akt prawny powszechnie obowiązujący, jakim jest rozporządzenie (art. 87 ust. 1 Konstytucji Rzeczypospolitej Polskiej), nie może być dokumentem niejawnym, a organ do spraw ochrony danych osobowych zdawał sobie sprawę z konieczności zachowania w tajemnicy działań prowadzonych wobec osób, o których informacje (których dane) znajdą się w wykazie. Rozstrzygnięcie powyższego zasygnalizowanego dylematu GIODO pozostawił do uznania projektodawcy, a w dalszej kolejności Parlamentu. Ponownie organ wskazał, iż w projekcie brak unormowań określających zasady dokonywania przez Agencję Bezpieczeństwa Wewnętrznego weryfikacji przydatności przetwarzanych przez nią danych. W projekcie nie powtórzono nawet rozwiązania przeniesionego do poprzednich projektów z ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym. (t.j. Dz.U. z 2014 r., poz. 1411 z późn. zm.). Zgodnie z nim, Agencja Bezpieczeństwa Wewnętrznego dokonywałaby weryfikacji potrzeby dalszego przetwarzania zebranych danych osobowych nie rzadziej niż co 5 lat.

Projektodawca zaproponował także, by Szef ABW niezwłocznie zawiadamiał Ministra Koordynatora Służb Specjalnych oraz Prokuratora Generalnego o zarządzeniu wobec osoby niebędącej obywatelem polskim niejawnego prowadzenia czynności określonych w ust. 1 komentowanego przepisu. GIODO skutecznie postulował, by w ramach systemu kontroli nad czynnościami prowadzonymi wobec osób, Prokurator Generalny miał dostęp do informacji, które doprowadziły do wydania zarządzenia wobec danej osoby.

Z brakiem zrozumienia po stronie projektodawcy spotkały się natomiast uwagi GIODO dotyczące rozszerzenia kompetencji Żandarmerii Wojskowej na **stosowanie wideomonitoringu i podsłuchu** oraz braku regulacji zasad informowania osób o objęciu monitoringiem oraz dostępu do nagrań, co ograniczać może prawa ujęte w art. 51 Konstytucji oraz przepisach ustawy o ochronie danych osobowych. W tym miejscu organ zwrócił uwagę na szerszy kontekst stosowania monitoringu wizyjnego przez organy państwa. Do Biura Generalnego Inspektora Ochrony Danych Osobowych nieprzerwanie płyną sygnały o potencjalnych naruszeniach prywatności osób obserwowanych, które z powodu braku regulacji ustawowej negatywnie wpływają na życie obywateli. W związku z tym Generalny Inspektor zwrócił się do Ministra Spraw

[82] Druk sejmowy nr 2295 (http://www.sejm.gov.pl/sejm7.nsf/PrzebiegProc.xsp?id=8E126F417E079EB7C1257CBA00279B51). DOLiS-033-337/13/TG/41198.

Wewnętrznych i Administracji z pytaniem, kiedy zostaną zakończone prace nad uregulowaniem monitoringu wizyjnego. Prowadzone od 2013 r. prace nad projektem założeń do ustawy o monitoringu wizyjnym[83] zostały przerwane wkrótce po zgłoszeniu w toku uzgodnień międzyresortowych i konsultacji publicznych uwag przez zainteresowane podmioty. Miało to miejsce w drugiej połowie 2014 r. Z odpowiedzi na interpelację poselską udzielonej przez Ministra[84] wynika, że celami uregulowania kwestii monitoringu wizyjnego są zapewnianie wysokiego poziomu bezpieczeństwa porządku publicznego oraz zapewnienie gwarancji przestrzegania praw i wolności konstytucyjnych osób obserwowanych i że zadanie to będzie realizowane w obecnej kadencji Sejmu. Jednocześnie brak jest konkretnych informacji o postępach w tym obszarze. Z drugiej strony Ministerstwo proponowało rozszerzenie katalogu podmiotów uprawnionych do stosowania obserwacji obywateli, co wpływa na prawo do prywatności osób obserwowanych. Prace nad ustawą o monitoringu wizyjnym powinny zostać przyśpieszone, aby zagwarantować przestrzeganie praw osób obserwowanych oraz wprowadzić pewność prawną co do zasad działania systemów monitoringu wizyjnego dla ich operatorów. Także Rzecznik Praw Obywatelskich[85] oraz Prezes Naczelnej Izby Kontroli[86] widzą potrzebę jak najszybszego unormowania tego obszaru. Podobne uwagi GIODO zgłosił do propozycji korzystania przez Straż Graniczną z systemów monitoringu wizyjnego znajdujących się na terenie portu lotniczego oraz zapisów z tych systemów.

Generalny Inspektor był także przeciwny propozycjom umożliwiającym Agencji Bezpieczeństwa Wewnętrznego blokowanie dostępu do danych informatycznych lub usług teleinformatycznych. Wątpliwość organu ds. ochrony danych osobowych budziły trzy kwestie. Po pierwsze, zbyt szerokie kryterium pozwalające na blokowanie treści. Ma to dotyczyć danych lub usług mających związek ze zdarzeniem o charakterze terrorystycznym. Tak szerokie spektrum może obejmować także dane ujęte w artykułach prasowych, blogach, nagraniach wideo itp. treści dostępne w publicznych sieciach komunikacyjnych. Po drugie, w projekcie nie wskazano, iż dla podmiotu zobowiązanego do zablokowania treści nie określono możliwości złożenia odwołania od postanowienia sądu czy zarządzenia albo żądania Szefa ABW. GIODO wskazał, że w projekcie powinna zostać przewidziana droga odwoławcza, aby zagwarantować możliwość weryfikacji decyzji o zablokowaniu treści. Po trzecie, w projekcie nie przewidziano narzędzia na wypadek potrzeby uzyskania dostępu do danych albo usługi przez inne osoby niż podejrzewane o udział w zdarzeniu terrorystycznym.

Na uznanie zasługują działania Ministra Cyfryzacji, który przeprowadził z udziałem GIODO **konsultacje nad proponowanymi zmianami przepisów Prawa telekomunikacyjnego, których mocą miano wprowadzić obowiązek rejestracji kart pre-paid**. Jest to tym bardziej istotne, że projektodawca – Minister Spraw Wewnętrznych i Administracji – nie przedstawił projektu do zaopiniowania organowi ds. ochrony danych osobowych. GIODO zwrócił uwagę, iż katalog danych abonenta (z

[83] http://legislacja.rcl.gov.pl/projekt/200701/katalog/200707#200707
[84] Odpowiedź na interpelację poselską nr 245 z 1.02.2016 r. http://sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=060D0780
[85] https://www.rpo.gov.pl/pl/content/mswia-o-pracach-legislacyjnych-zmierzajacych-do-uregulowania-kwestii-monitoringu-wizyjnego
[86] https://www.nik.gov.pl/aktualnosci/nik-o-miejskim-monitoringu-wizyjnym.html

dwoma wyłączeniami) podlegających obligatoryjnemu przekazaniu dostawcy poprzedzony został sformułowaniem „co najmniej" i zyskał w ten sposób charakter otwarty. Po drugie, organ negatywnie ocenił swobodę dostawcy w zakresie określania sposobu, w jaki abonent ma mu przekazać swoje dane, o których mowa w projektowanym art. 60b ust. 1 Prawa telekomunikacyjnego, gdyż rodzić może niebezpieczeństwo naruszenia praw abonenta. Byłby on bowiem zobligowany do przekazania („podania" według terminologii przyjętej w przepisie) swoich danych dostawcy, zaś dostawca może mu nakazać przekazanie tych danych w dowolny, wygodny dla siebie, sposób, w tym również taki, który nie zapewni ich bezpieczeństwa. Po trzecie, organ ds. ochrony danych osobowych wskazał, że w oparciu o projektowane przepisy Prawa telekomunikacyjnego nie tylko nie można ustalić, jak będzie się odbywać proces potwierdzania zgodności danych abonenta i jak w związku z tym procesem będą przetwarzane jego dane, lecz także – kto tego potwierdzenia może dokonywać. Po czwarte, zwrócił uwagę na kwestię osiągnięcia celu projektowanej zmiany Prawa telekomunikacyjnego – identyfikowanie wszystkich użytkowników usług telekomunikacyjnych. Jest to już dziś pośrednio możliwe poprzez weryfikację numerów IMEI. Ze względu na brak takiego obowiązku w innych krajach, należy się spodziewać wykorzystania przez osoby pragnące uniknąć identyfikacji kart SIM sprowadzonych z tych państw. W takim przypadku cel identyfikacyjny nie zostanie osiągnięty, a na usługobiorców i usługodawców telekomunikacyjnych nałożono istotny obowiązek utrudniający zachowanie w uzasadnionych przypadkach anonimowości komunikacji (informatorzy Policji, źródła informacji dziennikarzy i zwykli użytkownicy).

Większość z uwag Generalnego Inspektora Ochrony Danych Osobowych nie została przyjęta albo wyjaśniona przez projektodawcę. Ustawa weszła w życie 2 lipca 2016 r.

KRAJOWA ADMINISTRACJA SKARBOWA A ZASADA ADEKWATNOŚCI

Generalny Inspektor w toku prac sejmowych zgłaszał uwagi do projektów ustaw o Krajowej Administracji Skarbowej oraz Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej[87]. Uwagi ogólne dotyczyły wprowadzenia do obrotu prawnego przepisów o nowej administracji rządowej wykonującej zadania z zakresu realizacji dochodów z tytułu podatków itp. Powinny one zagwarantować bezpieczeństwo przetwarzania danych w związku z wykonywaniem obowiązków Krajowej Administracji poprzez poszanowanie przepisów art. 31 ust. 3, art. 47, 49 oraz 51 Konstytucji, przepisów ustawy o ochronie danych osobowych oraz prawa Unii Europejskiej w tym zakresie.

W projekcie określono otwarty katalog źródeł danych, z których mogą być pozyskiwane dane osobowe. Generalny Inspektor sugerował precyzyjne i wyczerpujące wskazanie źródeł danych, aby Szef KAS miał wyraźne podstawy prawne do przetwarzania informacji zbieranych w Centralnym Rejestrze Danych Podatkowych. W projekcie upoważniono organy KAS do zbierania i wykorzystywania informacji, w tym danych osobowych. **Negatywnie należy ocenić organ to, że nie wskazano zakresu danych niezbędnych dla realizacji tego zadania i celu.** Taką regulację Generalny Inspektor uznał za nieprawidłową i nieproporcjonalną, gdyż zgodnie z zasa-

[87] DOLiS-033-254/16.

dami ochrony danych katalog danych osobowych powinien być wyraźnie i wyczerpująco określony w przepisach rangi ustawowej.

Szczególną uwagę GIODO poświęcił przepisom o udostępnianiu danych z rejestrów publicznych i systemów teleinformatycznych za pomocą środków komunikacji elektronicznej. W obliczu problemów z dostępem uprawnionych podmiotów do rejestru PESEL stwierdził, iż obecnie stosowane w wielu ustawach regulacje są zbyt ogólne i nie zapewniają odpowiedniego poziomu ochrony i kontroli nad udostępnianymi danymi. Generalny Inspektor zasugerował, by Sejm rozważył wprowadzenie wyraźnego obowiązku kontroli przez organy KAS oraz podmiotów udostępniających informacje zakresu i częstotliwości udostępniania informacji, tak by uniemożliwić realizację nadmiernych i nieproporcjonalnych udostępnień. Szczególną uwagę sugerowano poświęcić porozumieniom i zgodom, na podstawie których ma dochodzić do dostępu do danych zgromadzonych w zbiorach danych.

GIODO wskazał również na brak przepisów o okresach przechowywania informacji zebranych w związku z prowadzeniem postępowań i przetwarzaniem informacji w Centralnym Rejestrze Danych Podatkowych i innych zbiorach danych. Brak unormowań w tym zakresie stanowi nieprawidłową regulację i ograniczenie praw osób, których dane dotyczą. Może także powodować postępujące rozszerzanie liczby informacji przetwarzanych przez organy KAS i wymagać dodatkowych środków na ich przechowywanie i prawidłowe zabezpieczenie, co może nieść za sobą konieczność wzrostu kosztów działalności.

W projekcie założono również, że informacje uzyskane przez organy KAS o obywatelach polskich były udostępniane na podstawie porozumienia Szefa KAS z instytucjami zagranicznymi lub międzynarodowymi organizacjami. Odnosząc się do tej kwestii GIODO wskazał, że przepis ten stanowi odejście od praktyki wymiany danych z organami innych państw albo organizacji na podstawie umów międzynarodowych. Dotychczas właściwe organy służb państwowych miały jedynie wykonywać postanowienia umów zawartych na poziomie międzyrządowym, a nie negocjować je i zawierać. W obliczu powyższego przypomniano o stanowisku Trybunału Konstytucyjnego w zakresie pozyskiwania i dalszego przetwarzania informacji. Trybunał w wyroku z 30 lipca 2014 r. (sygn. akt K 23/11) uznał za konieczne wprowadzenie proceduralnego wymogu, którym jest kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa. Status ustrojowy i zakres ustawowych kompetencji takiego organu ma gwarantować efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa. Konieczne jest, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to uznać należy za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej (jak wskazane zostało w cz. III, pkt 2 i 3 uzasadnienia wyroku – np. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05).

W projekcie wskazano, że dane osobowe przechowuje się przez okres, w którym są niezbędne dla realizacji ustawowych zadań, a weryfikacji dokonuje się nie rzadziej niż co

5 lat. GIODO uznał to rozwiązanie za naruszenie zasady ograniczenia czasowego ujętej w art. 26 ust. 1 pkt 4 ustawy, zgodnie z którą administrator ma obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania. Organ do spraw ochrony danych osobowych wskazywał, iż w projekcie brak jest unormowań określających zasady dokonywania przez organy KAS weryfikacji przydatności przetwarzanych przez nią danych.

Większość z powyższych uwag organu ds. ochrony danych osobowych niestety nie znalazła odzwierciedlenia w uchwalonej ustawie.

STATUS MINISTRA SPRAWIEDLIWOŚCI WOBEC DANYCH Z POSTĘPOWAŃ KARNYCH

W przypadku projektu ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw[88], Generalny Inspektor Ochrony Danych Osobowych zakwestionował propozycję zmiany ustawy z dnia 27 lipca 2001 roku – Prawo o ustroju sądów powszechnych[89].

W opinii organu do spraw ochrony danych osobowych zmiana ta prowadziła do nieuzasadnionej modyfikacji pozycji Ministra Sprawiedliwości w procesie przetwarzania danych na potrzeby postępowania karnego i jednocześnie pozostawała w widocznej sprzeczności z koncepcją nowelizacji art. 213 §1 a ustawy z dnia 6 czerwca 1997 roku – Kodeks postępowania karnego[90]. W artykule tym, Projektodawca odstąpił od obligatoryjnego pozyskiwania, przez organ prowadzący postępowanie karne, informacji z systemu teleinformatycznego ministra właściwego do spraw finansów publicznych dotyczących stosunków majątkowych i źródeł dochodu oskarżonego, w tym prowadzonych i zakończonych postępowań podatkowych, na rzecz rozwiązania fakultatywnego, w którym pobieranie takich danych następuje jedynie „w razie potrzeby". Ustalenie takiej „potrzeby" należy do organu prowadzącego postępowanie karne (prokuratora, innego organu prowadzącego postępowanie przygotowawcze, sądu). Konsekwentnie zatem to właściwy ze względu na stadium postępowania karnego organ prowadzący to postępowanie powinien być uznany za administratora danych przetwarzanych na podstawie tego przepisu. Decyduje on bowiem, że pozyskanie danych, o których mowa w art. 213 §1 a ustawy – Kodeks postępowania karnego, jest niezbędne dla osiągnięcia celu, jakim jest prawidłowość prowadzonego postępowania karnego.

Tymczasem – wbrew wyżej poczynionym ustaleniom – **Projektodawca uznał Ministra Sprawiedliwości za administratora danych uzyskanych z systemu teleinformatycznego ministra właściwego do spraw finansów publicznych** na podstawie art. 213 §1 a ustawy. Dał mu również prawo przetwarzania danych stron, pełnomocników uczestników postępowań sądowych i innych osób uczestniczących w postępowaniach karnych, uzyskanych z powyższego systemu teleinformatycznego.

Z koncepcją taką Generalny Inspektor Ochrony Danych Osobowych nie mógł się zgodzić, gdyż jej przyjęcie oznaczałoby, iż Minister Sprawiedliwości, który – w myśl przepisów ustawy – Kodeks postępowania karnego – uczestniczy w postępowaniu karnym jedynie

[88] DOLiS-033-33/16.
[89] Dz. U. Z 2016 r. poz. 2062, z późn. zm.
[90] Dz. U. Z 2016 r. poz. 1749, z późn. zm.

w niewielkim zakresie, zyskałby jako administrator danych[91] możliwość władczego decydowania o przetwarzaniu danych osób na potrzeby postępowania karnego. Zdaniem organu do spraw ochrony danych osobowych rozwiązanie takie byłoby niezgodne z przepisami procedury karnej oraz wykraczałoby poza – dopuszczony w wyroku Trybunału Konstytucyjnego z 14 października 2015 roku[92] – zakres kompetencji Ministra Sprawiedliwości do przetwarzania danych osobowych uczestników postępowań sądowych[93].

Uwagi Generalnego Inspektora Ochrony Danych Osobowych do projektu ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw były przedmiotem analizy na posiedzeniach sejmowej Podkomisji stałej do spraw nowelizacji prawa karnego w dniu 24 lutego 2016 roku oraz sejmowej Komisji Nadzwyczajnej do spraw zmian w kodyfikacjach w dniu 25 lutego 2016 roku. W wyniku tych prac oraz w następstwie uzgodnień poczynionych między przedstawicielami Ministerstwa Sprawiedliwości a przedstawicielami Generalnego Inspektor Ochrony Danych Osobowych Sejm Rzeczypospolitej Polskiej uchwalił kompromisowe brzmienie art. 175 c[94] ustawy – Prawo o ustroju sądów powszechnych[95]. Przepis ten w uzgodnionym z organem do spraw ochrony danych osobowych kształcie znalazł się w art. 10 pkt 5 ustawy z dnia 11 marca 2016 roku o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw[96].

CEIDG NIE JEST REJESTREM SŁUŻĄCYM UJAWNIANIU DŁUGÓW OSÓB FIZYCZNYCH PROWADZĄCYCH DZIAŁALNOŚĆ GOSPODARCZĄ

Choć w 2016 roku nie zostały zakończone prace legislacyjne[97] dotyczące projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw[98], to jest on wart odnotowania ze względu na charakter, zgłoszonych do niego przez organ do spraw ochrony danych osobowych, uwag. **Generalny Inspektor Ochrony Danych Osobowych nie mógł zgodzić się[99] przede wszystkim z propozycją wpisywania do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), a tym samym publicznego ujawniania w tej ewidencji informacji o zaległości w egzekucji świadczeń alimentacyjnych**, do zapłaty

[91] Podmiot, który zgodnie z art. 7 pkt 4 ustawy o ochronie danych osobowych decyduje o celach i środkach przetwarzania danych osobowych.

[92] Sygn. akt Kp 1/15.

[93] Sygn. akt Kp 1/15: „Minister Sprawiedliwości nie będzie zarządzać i decydować o przeznaczeniu danych zawartych w systemach teleinformatycznych, a jego zadania będą ograniczały się do stworzenia i obsługi samych systemów w warstwie technicznej." – teza 281 uzasadnienia wyroku; „Zaskarżony przepis ten nie przyznaje tym samym Ministrowi Sprawiedliwości ogólnej, nieograniczonej kompetencji do przetwarzania danych stron, pełnomocników i innych osób uczestniczących w postępowaniach sądowych zawartych w tych systemach." – teza 285 uzasadnienia wyroku.

[94] W projekcie ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw oznaczonego jako art. 175 b ustawy – Prawo o ustroju sądów powszechnych.

[95] „Art. 175c § 1. Minister Sprawiedliwości jest administratorem systemu służącego do przetwarzania danych osobowych uzyskanych z systemu teleinformatycznego, o którym mowa w art. 213 § 1a Kodeksu postępowania karnego. Do przetwarzania danych osobowych nie stosuje się przepisu art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Art. 175c § 2. Minister Sprawiedliwości przetwarza dane osób uzyskane z systemu teleinformatycznego, o którym mowa w art. 213 §1a Kodeksu postępowania karnego, wyłącznie w zakresie niezbędnym do realizacji zadania, o którym mowa w § 1.".

[96] Dz. U. Z 2016 r. poz. 437.

[97] Według informacji zamieszczonej przez Rządowe Centrum Legislacji na stronie internetowej www.rcl.gov.pl zakładka „Rządowy proces legislacyjny" ostatnie prace legislacyjne dotyczące projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw miały miejsce w dniu 6 grudnia 2016 roku.

[98] DOLiS-033-518/16.

[99] Choć uznaje za wysoce naganne i społecznie szkodliwe zjawisko uporczywej niealimentacji.

których zobowiązany jest przedsiębiorca, za okres dłuższy niż 6 miesięcy. Generalny Inspektor Ochrony Danych Osobowych jednoznacznie negatywnie ocenia postawę tych osób, wśród których znajdują się też przedsiębiorcy, które nie wykonują obciążającego ich obowiązku alimentacyjnego. Jednakże zwalczanie szkodliwego zjawiska społecznego nie powinno – w opinii organu do spraw ochrony danych osobowych – odbywać się przy użyciu środków nieprawidłowych i nieadekwatnych, czy wręcz wątpliwych w kwestii ich skuteczności.

CEIDG nie jest rejestrem służącym ujawnianiu długów osób fizycznych prowadzących działalność gospodarczą. Zgodnie bowiem z ustawą o swobodzie działalności gospodarczej zadaniem CEIDG jest m.in. ewidencjonowanie przedsiębiorców będących osobami fizycznymi, udostępnianie informacji o przedsiębiorcach i innych podmiotach w zakresie wskazanym w ustawie. Tymczasem zobowiązania alimentacyjne osoby fizycznej prowadzącej działalność gospodarczą nie pozostają w jakimkolwiek związku z prowadzoną przez tę osobę działalnością gospodarczą. Ustawodawca nie posiada całkowitej swobody w zakresie zmiany celów prowadzenia publicznego rejestru. Skoro zatem CEIDG jest rejestrem powstałym dla celów ewidencyjnych[100], to nie może być przekształcony w rejestr długów osób fizycznych prowadzących działalność gospodarczą bez wykazania przez Projektodawcę, że taka zmiana spełnia przesłankę „niezbędności w demokratycznym państwie prawnym”[101]. Tę „niezbędność” uznać zaś należy za wysoce wątpliwą skoro w prawie polskim istnieją już inne środki służące dyscyplinowaniu dłużników alimentacyjnych, jak na przykład przekazywanie do biur informacji gospodarczej informacji gospodarczej o zobowiązaniu dłużnika alimentacyjnego.

Powstaje pytanie o cel takiej regulacji. W**edług Generalnego Inspektora Ochrony Danych Osobowych celem tym jest stygmatyzacja przedsiębiorcy zalegającego z zapłatą świadczeń alimentacyjnych**. Taka celowa stygmatyzacja określonej grupy osób przez władze publiczne stanowi zaś naruszenie art. 30 Konstytucji Rzeczypospolitej Polskiej, zwłaszcza że z ogółu dłużników alimentacyjnych[102] ustawodawca arbitralnie wybrał akurat przedsiębiorców i to wobec nich chce zastosować tak drastyczny środek, jakim jest ujawnienie informacji o ich długach prywatnych w rejestrze służącym innym celom. W oparciu o wyżej zaprezentowane konstatacje organ do spraw ochrony danych osobowych wnosił o wykreślenie z projektu tej zmiany.

PESEL POD SZCZEGÓLNĄ OCHRONĄ

Z punktu widzenia – określonych w ustawie o ochronie danych osobowych – zasad ochrony tych danych, a w szczególności zasady adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane[103], **Generalny Inspektor Ochrony Danych Osobowych zakwestionował także przetwarzanie numerów PESEL dyrektorów oddziałów Zakładu Ubezpieczeń Społecznych i dyrektorów izb celnych w ramach list prowadzonych przez ministra właściwego do spraw finansów publicznych** na podstawie ustawy z dnia 17 czerwca 1966

[100] Art. 23 ust. 3 pkt 1 ustawy o swobodzie działalności gospodarczej.
[101] Art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej.
[102] Czyli osób zachowujących się w sposób niezgodny z zasadami współżycia społecznego.
[103] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

roku o postępowaniu egzekucyjnym w administracji[104]. W opinii organu do spraw ochrony danych osobowych w tym celu dana osobowa, jaką jest numer PESEL, jest całkowicie zbędna. Co więcej – dana ta nie jest przetwarzana w ramach, służącej dokładnie temu samemu celowi, listy naczelników urzędów skarbowych, zastępców naczelników urzędów skarbowych oraz osób wyznaczonych do realizacji zadań naczelnika urzędu skarbowego, przewidzianej w ustawie z dnia 10 lipca 2015 roku o administracji skarbowej[105]. Dlatego Generalny Inspektor Ochrony Danych Osobowych wnosił o usunięcie z proponowanych przepisów sformułowań: „numer PESEL".

Co więcej, w związku przyjęciem przez Projektodawcę – art. 3 a oraz następne ustawy z dnia 20 sierpnia 1997 roku o Krajowym Rejestrze Sądowym[106] – rozwiązania, zgodnie z którym akta rejestrowe podmiotów wpisanych do Krajowego Rejestru Sądowego będą udostępniane za pośrednictwem systemu teleinformatycznego utrzymywanego przez Ministerstwo Sprawiedliwości, organ do spraw ochrony danych osobowych przypomniał[107], że taki sposób udostępniania akt rejestrowych oznaczać będzie znaczącą ingerencję w prywatność obywateli. Liczne dane osobowe znajdujące się w aktach rejestrowych staną się nie tylko jawne, ale także powszechnie dostępne, co wywoła daleko idące skutki prawne. Będą dostępne dla podmiotów z całego świata przez czas nieograniczony, nie będą mogły być skutecznie usunięte, w przypadku gdy osoba, której one dotyczą, przestanie zajmować stanowisko/pełnić funkcję będące/będącą przyczyną wpisu oraz będą mogły być pozyskiwane bez żadnych ograniczeń przez osoby fizyczne i podmioty gospodarcze, a następnie wykorzystywane przez te osoby i podmioty w dowolnych celach i w dowolny sposób. Projektodawca musi mieć świadomość powyższych konsekwencji, zaś rolą Generalnego Inspektora Ochrony Danych Osobowych, jako organu do spraw ochrony danych osobowych[108], jest te konsekwencje uświadamiać i przed nimi ostrzegać. Skoro[109] Projektodawca dalej optuje za rozwiązaniem polegającym na umożliwieniu dostępu do akt rejestrowych podmiotów wpisanych do Krajowego Rejestru Sądowego za pośrednictwem systemu teleinformatycznego przez siebie utrzymywanego, bierze na siebie pełną odpowiedzialność za to rozwiązanie, w tym również za takie ryzyka jak kradzież tożsamości, profilowanie etc. To Projektodawca dokonał wyważenia między chronionymi wartościami jakimi są bezpieczeństwo obrotu prawnego oraz prawo do prywatności osób fizycznych i zdecydował, iż bezpieczeństwu obrotu prawnego należy w tej sytuacji nadać priorytet. Ocenę tę organ do spraw ochrony danych osobowych uszanował nie przestając wszakże akcentować skutków, jakie przyjęte w Krajowym Rejestrze Sądowym regulacje rodzić będą w sferze ochrony danych osobowych.

Projektodawca nie ustosunkował się w okresie sprawozdawczym na piśmie do uwag Generalnego Inspektora Ochrony Danych

[104] Dz. U. z 2016 r. poz. 599, z późn. zm.
[105] Uchylonej z dniem 1 marca 2017 roku przez art. 159 pkt 4 ustawy z dnia 16 listopada 2016 roku – Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej (Dz. U. Z 2016 r. poz. 1948, z późn. Zm.).
[106] Dz. U. z 2017 r. poz. 700, z późn. zm.
[107] Kwestia ta była już podnoszona w pismach Generalnego Inspektora Ochrony Danych Osobowych skierowanych na etapie projektu założeń do Pana Marcina Warchoła – Podsekretarza Stanu w Ministerstwie Sprawiedliwości z dnia 9 marca 2016 roku o sygn. DOLiS-033-284/14/TG/16213/16 i Pana Łukasza Piebiaka – Podsekretarza Stanu w Ministerstwie Sprawiedliwości z dnia 23 marca 2016 roku o sygn. DOLiS-033-284/14/TG/20931/16.
[108] Art. 8 ust. 1 ustawy o ochronie danych osobowych.
[109] Mając już od etapu projektu założeń pełną wiedzę o nieuniknionych następstwach przyjętych unormowań.

Osobowych zgłoszonych do projektu ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw.

DANE MEDYCZNE Z REJESTRU NOWOTWORÓW WYMAGAJĄ REGULACJI USTAWOWEJ

Z opiniowanych w 2016 roku projektów rozporządzeń zasługuje na wspomnienie projekt rozporządzenia Ministra Zdrowia w sprawie Krajowego Rejestru Nowotworów[110].

Zapoznawszy się z tym projektem organ do spraw ochrony danych osobowych stwierdził bowiem, iż nie wykonuje on prawidłowo delegacji zawartej ustawie o systemie informacji w ochronie zdrowia[111]. Wbrew jednoznacznemu brzmieniu art. 20 ust. 1 pkt 5 ustawy o systemie informacji w ochronie zdrowia **projekt nie określa zakresu i rodzaju danych przetwarzanych w Krajowym Rejestrze Nowotworów**.

Zamiast wymaganego katalogu danych mających być przetwarzanymi w Krajowym Rejestrze Nowotworów, projekt odsyła w tej kwestii do wzoru karty zgłoszenia nowotworu złośliwego, określonej w rozporządzeniu Prezesa Rady Ministrów wydanym na podstawie delegacji z ustawy z dnia 29 czerwca 1995 roku o statystyce publicznej[112]. Rozwiązanie takie nie mogło być zaakceptowane przez Generalnego Inspektora Ochrony Danych Osobowych, gdyż **przetwarzanie danych szczególnie chronionych, a do takiej kategorii należą, zawarte w rejestrach medycznych – w tym Krajowym Rejestrze Nowotworów – dane o stanie zdrowia, odbywać się powinno na podstawie przepisów szczególnych rangi ustawowej stwarzających przy tym pełne gwarancje ochrony takich danych. Wyjątek taki**[113] nie może być interpretowany rozszerzająco i niejako legalizować przetwarzania danych szczególnie chronionych na podstawie przepisów rozporządzeń wydanych w oparciu o inne ustawy niż ustawa o systemie informacji w ochronie zdrowia. Do takiej zaś swoistej legalizacji przepisów wykonawczych do ustawy o statystyce publicznej prowadziłoby, zaproponowane w projekcie, brzmienie przepisów. Co więcej, skoro ustawodawca - w ustawie o systemie informacji w ochronie zdrowia - zdecydował się powierzyć ministrowi właściwemu do spraw zdrowia[114] określenie zakresu i rodzaju danych przetwarzanych w Krajowym Rejestrze Nowotworów, to minister ten nie może cedować tego obowiązku na inny podmiot – art. 92 ust. 2 w zw. z ust. 1 Konstytucji Rzeczypospolitej Polskiej. Do takiej zaś sytuacji doszłoby w przypadku przyjęcia projektu w zaproponowany kształcie. Zgodnie bowiem z ustawą o statystyce publicznej rozporządzenie wykonawcze kreujące wzór karty zgłoszenia nowotworu złośliwego wydaje Prezes Rady Ministrów, nie zaś Minister Zdrowia. Tym samym, unormowanie przewidziane w projekcie prowadziłoby do powstania stanu prawnego, w którym to Prezes Rady Ministrów, a nie Minister Zdrowia, decydowałby o zakresie danych przetwarzanych w Krajowym Rejestrze Nowotworów. W opinii Generalnego Inspektora Ochrony Danych Osobowych rozwiązanie takie budziłoby wątpliwości co do

[110] DOLiS-033-6/16.
[111] Dz. U. z 2016 r. poz. 1535, z późn. zm.
[112] Dz.U. z 2016 r., poz. 1068 z późn. zm.
[113] W myśl zasady „exceptiones non sunt extendendae".
[114] Ministrowi Zdrowia – §1 ust. 1 i 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 roku w sprawie szczegółowego zakresu działania Ministra Zdrowia (Dz. U. Z 2015 r. poz. 1908).

zgodności z Konstytucją Rzeczypospolitej Polskiej.

Z wskazanych wyżej przyczyn organ do spraw ochrony danych osobowych nie zaakceptował projektu rozporządzenia Ministra Zdrowia w sprawie Krajowego Rejestru Nowotworów i wnosił o jego poprawienie.

Podpisane przez Ministra Zdrowia rozporządzenie Ministra Zdrowia z dnia 24 sierpnia 2016 roku w sprawie Krajowego Rejestru Nowotworów[115] uwzględnia uwagi Generalnego Inspektora Ochrony Danych Osobowych i w §3 zawiera enumeratywny katalog danych oraz informacji przetwarzanych w Krajowym Rejestrze Nowotworów.

INFORMACJE O SZCZEPIENIACH W SANEPIDZIE

Kolejnym z opiniowanych przez Generalnego Inspektora projektów legislacyjnych był projekt ustawy o zmianie ustawy o Państwowej Inspekcji Sanitarnej oraz niektórych innych ustaw [116].

W pierwszej kolejności Generalny Inspektor zwrócił się z prośbą do Ministra o rozważenie uwzględnienia w zmienianych ustawą o zmianie ustawy o Państwowej Inspekcji Sanitarnej oraz niektórych innych ustaw ustawach przepisach zapisów, które **będą legalizowały przekazywanie informacji do państwowego powiatowego inspektora sanitarnego o osobach, które nie poddały się obowiązkowym szczepieniom ochronnym**.

Wskazał, iż do Biura GIODO docierają liczne skargi osób niezadowolonych z praktyk stosowanych przez podmioty lecznicze, polegających na przekazywaniu państwowemu powiatowemu inspektorowi sanitarnemu danych osobowych osób niezaszczepionych co w obecnym stanie prawnym nie jest wyraźnie uregulowane w przepisach prawa. Problem ten dotyczy przede wszystkim przekazywania danych osobowych dzieci, których rodzice świadomie nie zdecydowali się poddać je obowiązkowym szczepieniom ochronnym. W związku z powyższym GIODO zaproponował wprowadzenie stosownych zmian w zakresie przekazywania danych osobowych osób niezaszczepionych państwowym powiatowym inspektorom sanitarnym jednocześnie z wprowadzaniem nowych regulacji objętych przedmiotowym projektem.

GIODO poinformował, iż w art. 27 ustawy o ochronie danych osobowych przewidziane zostały zasady postępowania z danymi osobowymi podlegającymi szczególnej ochronie[117]. Zaznaczył, iż zgodnie ustawą z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. z 2013 r. poz. 947), osoby przeprowadzające szczepienia ochronne sporządzają sprawozdania z przeprowadzonych obowiązkowych szczepień ochronnych oraz sprawozdania ze stanu zaszczepienia osób objętych profilaktyczną opieką zdrowotną, które przekazują państwowemu powiatowemu inspektorowi sanitarnemu. Wskazany przepis nie uprawnia wprost do przekazywania państwowym powiatowym inspektorom sanitarnym informacji zawierają-

[115] Dz. U. z 2016 r. poz. 1362.
[116] DOLiS-033-451/16.
[117] Zgodnie z treścią ust. 1. powołanego przepisu, co do zasady zabrania się przetwarzania danych ujawniających m.in. dane o stanie zdrowia. Zgodnie z ust. 2 powołanego artykułu ustawy o ochronie danych osobowych, przetwarzanie danych, o których mowa w ust.1 jest jednak dopuszczalne, jeżeli przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą i stwarza pełne gwarancje ich ochrony (art. 27 ust.2 pkt 2 ustawy).

cych dane osobowe niezaszczepionych pacjentów, bowiem mowa jest tylko o „stanie zaszczepienia”[118].

Zestawienia danych osób, które nie poddały się szczepieniom tworzone są na podstawie nieprecyzyjnego i niewystarczającego sformułowania „imienny wykaz” o którym mowa w załączniku nr 4 do rozporządzenia Ministra Zdrowia z dnia 18 sierpnia 2011 r. w sprawie obowiązkowych szczepień (Dz.U. 2016 r. poz. 849). Konieczne jest zatem określenie zakresu danych osób oraz kategorii osób, które mają być przekazywane celem weryfikacji przez państwowego powiatowego inspektora sanitarnego.

GIODO wskazywał, że przetwarzanie danych osobowych szczególnie chronionych, aby było legalne, musi wynikać z przepisów rangi ustawy, nie zaś rozporządzenia czy załącznika do rozporządzenia. Organ zasugerował zatem, że w ustawie powinno zostać wskazane wprost – jakie dane i w jakim zakresie oraz w jakim celu mają być przekazywane. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym[119]. Stąd regulacje prawne muszą precyzyjnie określać zakres danych osobowych oraz cele, dla których będą one przetwarzane[120].

GIODO postulował zatem, że jeżeli wprowadzany jest obowiązek poddania się szczepieniom oraz istnieje konieczność weryfikacji osób niezaszczepionych to należy stworzyć regulacje ustawowe o charakterze zupełnym, które kompleksowo będą stanowić o zasadach przetwarzania danych osobowych w tym zakresie.

Generalny Inspektor zauważył także, iż projektodawca proponował zwiększyć uprawnienia Głównego Inspektora Sanitarnego o rejestrowanie obrazu lub dźwięku. Generalny Inspektor Ochrony Danych Osobowych wskazał, iż konieczne byłoby doprecyzowanie tej kwestii w przepisach ustawy oraz wskazanie, w jakim celu i zakresie obraz i dźwięk miałby być rejestrowany, w jaki sposób będzie spełniony obowiązek informacyjny wobec osób, których dane będą przetwarzane w związku z dokonywaniem przez Państwową Inspekcję Sanitarną rejestrowania obrazu lub dźwięku, a także w jaki sposób zarejestrowane dane będą wykorzystywane i jak długo przechowywane.

Projekt ustawy zakładał również nadanie Państwowej Inspekcji Sanitarnej uprawnienia do żądania okazania dokumentów i udostępniania danych, w tym sporządzania niezbędnych

[118] Dyspozycja § 13 rozporządzenia Ministra Zdrowia z dnia 18 sierpnia 2011 r. w sprawie obowiązkowych szczepień który stanowi natomiast, że kwartalne sprawozdanie z przeprowadzonych obowiązkowych szczepień ochronnych (Dz.U. 2016 r. poz. 849)., którego wzór jest określony w załączniku nr 4 do rozporządzenia, jest sporządzane i przekazywane przez osoby przeprowadzające obowiązkowe szczepienia ochronne państwowemu powiatowemu inspektorowi sanitarnemu, w terminie 7 dni po zakończeniu kwartału, za pomocą środków komunikacji elektronicznej albo listem poleconym.

[119] Zgodnie z art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw. Ponadto artykuł 51 ust. 1 Konstytucji Rzeczypospolitej Polskiej stanowi, iż nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

[120] W tym miejscu GIODO zwrócił uwagę na stanowisko Trybunału Konstytucyjnego, wyrażone w postanowieniu z dnia 31 stycznia 2007 r. (sygnatura S 1/2007)[120]. 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.

ich kopii oraz urzędowego tłumaczenia na język polski dokumentów i danych sporządzonych w języku obcym, dlatego też Generalny Inspektor wskazał, że w przepisach ustawy należałoby szczegółowo wskazać, jakich konkretnie danych i dokumentów może żądać Państwowy Inspektor Sanitarny.

W odpowiedzi na uwagi GIODO Główny Inspektor Sanitarny poinformował, iż uwagi Generalnego Inspektora Ochrony Danych Osobowych w zakresie konieczności stworzenia precyzyjnego katalogu danych osób uchylających się od szczepień ochronnych, które mogą być przekazywane do państwowych powiatowych inspektorów sanitarnych zostaną uwzględnione w projekcie ustawy o zmianie ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi.

Odnosząc się natomiast do uwagi dotyczącej projektowanych zapisów związanych z rozszerzeniem kompetencji kontrolnych organów Państwowej Inspekcji Sanitarnej w zakresie uprawnień do rejestrowania obrazu i dźwięku, Główny Inspektor Sanitarny poinformował, iż kwestie związane z obowiązkiem informacyjnym wobec osób, których dane będą przetwarzane w związku z rejestrowaniem obrazu i dźwięku, sposób wykorzystania zarejestrowanych danych oraz długość ich przechowywania zostaną uregulowane w rozporządzeniu ministra właściwego do spraw zdrowia. W toku dalszych prac legislacyjnych Generalny Inspektor wyraził wątpliwości co do rozwiązania polegającego na uregulowaniu tych kwestii w przepisach rangi rozporządzenia. [121]

W kwestii związanej z projektowanym przepisem, który miałby uprawniać organy Państwowej Inspekcji Sanitarnej do żądania okazania dokumentów i udostępniania danych, w tym sporządzania niezbędnych ich kopii oraz urzędowego tłumaczenia na język polski dokumentów i danych sporządzonych w języku obcym, Główny Inspektor Sanitarny wyjaśnił, iż organy Państwowej Inspekcji Sanitarnej w toku przeprowadzanej urzędowej kontroli u przedsiębiorców branży spożywczej mogą żądać tłumaczenia dokumentów sporządzonych w języku obcym dotyczących żywności np. specyfikacji produktów czy wyników badań w celu wyjaśnienia sprawy (art. 75 § 1 k.p.a.) tj. np. prawidłowego przeprowadzenia czynności kontrolnych dotyczących ustalenia czy kontrolowany przedsiębiorca branży spożywczej spełnia wymagania wynikające z przepisów prawa żywnościowego[122]. Generalny Inspektor Ochrony Danych Osobowych przyjął argumentację, iż dostęp do dokumentacji jest niezbędny w celu realizowania kontroli przez Państwową Inspekcję Sanitarną w trybie przepisów ustawy z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia. Przepisy jednak powinny wskazywać zakres danych, które będą przetwarzane. Generalny Inspektor

[121] W tym miejscu GIODO przypomniał stanowisko wyrażone przez Trybunał Konstytucyjny w uzasadnieniu postanowienia z dnia 31 stycznia 2007 roku (Sygn. akt S 1/2007).Także art. 31 ust. 3 Konstytucji wymaga regulacji ustawowej w tych wszystkich unormowaniach, które dotyczą ograniczeń konstytucyjnych praw i wolności jednostki. W takim wypadku zakres materii pozostawianych do unormowania w rozporządzeniu musi być węższy niż zakres materii ogólnie dozwolony na tle art. 92 ust. 1 Konstytucji. Artykuł 31 ust. 3 Konstytucji silniej bowiem akcentuje konieczność szerszego unormowania rangi ustawowej i zawęża pole regulacyjne pozostające dla rozporządzenia.

[122] Główny Inspektor Sanitarny dodał również, iż zgodnie z art. 4 ustawy z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia do postępowania przeprowadzanego przez organy urzędowej kontroli żywności stosuje się przepisy Kodeksu postępowania administracyjnego, jeżeli przepisy ustawy nie stanowią inaczej. a tym samym do czynności związanych z przeprowadzaniem urzędowej kontroli u przedsiębiorców branży spożywczej przez organy urzędowej kontroli żywności – organy Państwowej Inspekcji Sanitarnej na podstawie art. 73 ustawy z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia – zastosowanie będą miały także przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Do oceny danej sprawy organ kontrolny jest obowiązany w sposób wyczerpujący zebrać i rozpatrzeć dokumentację sprawy. W takiej sytuacji, aby właściwie ocenić daną sprawę konieczne jest przedłożenie przez stronę tłumaczenia dokumentów właściwych ze względu na przedmiot kontroli.

zwrócił uwagę również na kwestię kopiowania dokumentów [123].

Główny Inspektor Sanitarny pismem z dnia 17 listopada 2016 r.[124] poinformował, iż po zakończeniu konsultacji społecznych oraz dokonaniu szczegółowej analizy uwag do projektu odstąpiono od propozycji rejestrowania obrazu i dźwięku przez Państwową Inspekcję Sanitarną. Poinformował również, iż uwzględniona została uwaga Generalnego Inspektora Ochrony Danych Osobowych dotycząca zakresu danych, jakie będą przetwarzane na potrzeby kontroli w związku z projektowanym uprawnieniem dla organów Państwowej Inspekcji Sanitarnej do żądania od podmiotu kontrolowanego okazania dokumentów i udostępniania danych.

Prace nad projektem nie zostały zakończone w 2016 r. i trwają do chwili obecnej.

ZASADY OCHRONY DANYCH W TWORZENIU KRAJOWYCH SYSTEMÓW TELEINFORMATYCZNYCH

GIODO wniósł obszerne uwagi do projektu ustawy – przepisy wprowadzające ustawę – Prawo oświatowe oraz do projektu ustawy Prawo oświatowe [125].

W projekcie ustawy zastrzeżenia organu do spraw ochrony danych osobowych wzbudziła delegacja ustawowa zawarta w Karcie Nauczyciela, w której minister właściwy do spraw oświaty udostępnia **system teleinformatyczny, umożliwiający dyrektorowi szkoły ustalenie, czy numer PESEL danego nauczyciela lub osoby ubiegającej się o zatrudnienie na stanowisku nauczyciela** znajduje się w Centralnym Rejestrze Orzeczeń Dyscyplinarnych (CROD). Zasadnicze wątpliwości Generalnego Inspektora dotyczyły systemu teleinformatycznego, w szczególności czy będzie on tożsamy z CROD, czy będzie to nowy system – odrębny od CROD oraz jaki zakres informacji zostanie udostępniony dyrektorowi szkoły poprzez powyższy system, mając na uwadze, iż CROD zawiera wiele danych wrażliwych, które nie są tożsame z informacjami udostępnianymi na wniosek dyrektora.

Wątpliwości organu do spraw ochrony danych osobowych wzbudziły jednocześnie liczne przepisy, w których zobligowano osobę prawną niebędącą jednostką samorządu terytorialnego, bądź osobę fizyczną do przedłożenia organowi jednostki samorządu terytorialnego wykazu nauczycieli przewidzianych do zatrudnienia wraz z informacją o ich kwalifikacjach.

GIODO wskazał również, iż przepisy projektu nie określają sposobu, w jaki będą przekazywane informacje o aktualnym stanie i zmianach w ewidencji dzieci i młodzieży oraz zakresu danych, jaki będzie zawierać ewidencja. W szczególności zwrócił uwagę na brak wskazania zakresu przetwarzanych danych osobowych dzieci i młodzieży, jaki będą zawierały przedmiotowe ewidencje, a także zakresu informacji, jakie wójt gminy (burmistrz lub prezydent miasta) jest obowiązany przeka-

[123] Z punktu widzenia zasad wynikających z przepisów ustawy o ochronie danych osobowych istotne jest, aby gromadzenie danych (odbywające się np. poprzez kopiowanie dokumentów) było zgodne z prawem i nie prowadziło do zebrania danych w zakresie szerszym, niż to jest konieczne dla realizacji celu, w jakim dane są przetwarzane. Zgodnie z zasadą legalizmu wyrażoną w art. 26 ust.1 pkt 1, dane powinny być przetwarzane zgodnie z prawem. Zgodnie zaś z zasadą adekwatności, wynikającą z art. 26 ust. 1 pkt 3 ustawy, o ochronie danych osobowych dane powinny być adekwatne do celów, w jakich są przetwarzane[123]. Zasady te powinny być natomiast respektowane przez projektodawcę odpowiedzialnego za stworzenie właściwych przepisów prawa, które będą regulować określoną materię prawną w sposób klarowny i wyczerpujący.

[124] Sygnatura GIS-BI-OI-073-00012/JKM,AZ/16.

[125] DOLIS-033-437/16.

zywać dyrektorom szkół. Dla wyznaczenia zarówno zakresu informacji, jakie zawierać ma ewidencja, jak i zakresu informacji, jakie mają być przekazywane dyrektorom szkół, znaczenie mają zasady legalizmu, celowości i adekwatności przetwarzania danych osobowych zawarte w art. 26 ust. 1 pkt 1-3 ustawy o ochronie danych osobowych[126]. Jednocześnie Generalny Inspektor wskazał, iż proces przetwarzania danych, w tym przekazywania danych osobowych, powinien przebiegać zgodnie z przepisami o ochronie danych osobowych, w tym dane powinny być w odpowiedni sposób zabezpieczone. Reasumując, projektodawca powinien określić w przepisach opiniowanej ustawy zakres, cel i sposób przekazywania, w tym przetwarzania danych osobowych, ściśle odpowiadające kontroli spełnienia obowiązku szkolnego, w tym gromadzeniu w ewidencjach i wymianie informacji pomiędzy wójtem (burmistrzem lub prezydentem miasta) a dyrektorami szkół.

Generalny Inspektor Ochrony Danych Osobowych zgłosił również wątpliwość co do zakresu danych osobowych, do których ma mieć dostęp organ sprawujący nadzór pedagogiczny; odniósł się także do kwestii elektronicznej platformy nadzoru. Ponieważ elektroniczna platforma nadzoru ma służyć do zapewnienia sprawności i efektywności nadzoru pedagogicznego, to przepisy rangi ustawy powinny regulować zasadnicze kwestie dotyczące prowadzenia tejże platformy i przetwarzanie przy jej pomocy danych osobowych. W szczególności zaś: katalog danych dostępnych przez platformę, okres przechowywania tych danych, zasady udostępniania informacji oraz krąg podmiotów mających dostęp do danych[127].

GIODO wyraził również wątpliwość dotyczącą sposobu zasilania platformy elektronicznej oraz zakresu i formy przekazywanych danych – wskazując, że kwestią wymagającą doprecyzowania jest przede wszystkim to, z jaką częstotliwością dane miałyby być przekazywane do centralnego rejestru i w jaki sposób aktualizowane, a także w jakiej formie dokonywane będą sprostowania nieprawdziwych informacji, tzn. czy będą one usuwane czy nadpisywane (jest to istotne z punktu widzenia zapewnienia prawdziwości gromadzonych danych).

W odniesieniu do przepisów regulujących katalog kryteriów, jakie musi spełniać osoba ubiegająca się o stanowisko dyrektora placówki, wprowadzających możliwość określenia przez ministra właściwego dodatkowych wymagań, jakim powinna odpowiadać osoba zajmująca stanowisko dyrektora, GIODO zwrócił uwagę, że jeżeli projektodawca ma w niniejszym przypadku na celu rozszerzenie katalogu wymaganych kryteriów, których spełnienie i wykazanie miałoby się wiązać z przetwarzaniem danych osobowych kandydata, to nie jest to dopuszczalne mocą przepisów rangi aktu wykonawczego. Jedynie bowiem akt rangi ustawy może wprowadzać prawo przetwarzania danych informacji oraz nakładać na osobę obowiązek udostępniania informacji o osobie (por. art. 31 ust. 3 i art. 51 Konstytucji RP).

Generalny Inspektor odniósł się także do przepisów regulujących funkcjonowanie rady rodzi-

[126] Zakres przetwarzania danych musi odpowiadać celowi przetwarzania danych osobowych przez wskazane organy polegającymi na kontroli spełnienia obowiązku szkolnego. Zarówno zakres przetwarzanych danych osobowych w ewidencjach, jak i zakres danych przekazywanych dyrektorom szkół powinien być wskazany wyczerpująco i wprost w przepisach powszechnie obowiązujących opiniowanej ustawy.

[127] Potwierdzenie powyższego zawarte jest w stanowisku Trybunału Konstytucyjnego, wyrażonego 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".

ców, które związane jest w nierozerwalny sposób z przetwarzaniem danych osobowych, w tym także szczególnie chronionych, przy czym mogą to być zarówno dane uczniów i ich rodziców czy opiekunów prawnych, jak i grona pedagogicznego. Generalny Inspektor zwrócił uwagę, iż nie jest sprecyzowane, kto jest odpowiedzialny za przetwarzanie danych osobowych, którymi dysponuje rada rodziców oraz w jaki sposób spełnia ona obowiązki wynikające z przepisów dotyczących przetwarzania danych osobowych (np. obowiązek informacyjny, obowiązek respektowania prawa do kontroli procesu przetwarzania danych osobowych, obowiązek zabezpieczenia, archiwizacji czy obowiązek usunięcia danych zbędnych). GIODO – wobec powyższego – zasugerował stworzenie regulacji, która wprowadziłaby wprost obowiązek zapewnienia przez szkołę administracyjno-organizacyjnej obsługi funkcjonowania rady rodziców.

Organ do spraw ochrony danych osobowych wskazał także, iż kryterium związane z przetwarzaniem informacji o osobach (dzieciach i/lub ich rodzicach / opiekunach prawnych) musi wynikać z przepisów rangi ustawy, gdyż tylko mocą takiego przepisu można nakładać prawo przetwarzania takich informacji, jak i obowiązek ich udostępnienia (por. art. 31 ust. 3 i art. 51 Konstytucji RP). Zasada ta powinna znaleźć zastosowanie także w związku z określaniem praw i obowiązków dzieci oraz przypadków, w których dyrektor przedszkola może skreślać dziecko z listy wychowanków, co bez wątpienia wiązać się będzie z przetwarzaniem informacji zindywidualizowanych (danych osobowych) o dzieciach i/lub ich rodzicach czy opiekunach prawnych, zwłaszcza o ile będzie to pozostawać w związku z danymi szczególnie chronionymi.

GIODO wskazał ponadto, iż w ustawie o systemie oświaty zawarta jest kompleksowa regulacja postępowania rekrutacyjnego w tym dotycząca sposobu postępowania z dokumentacją kwalifikacyjną, która została wypracowana we współpracy z organem do spraw ochrony danych osobowych. Organ do spraw ochrony danych osobowych zwrócił uwagę, iż w projekcie brak jest uzasadnienia dla rezygnacji z tego rozwiązania oraz dla przeniesienia części regulacji ustawowej do przepisów rangi rozporządzenia. W opinii GIODO, istotne jest ponowne rozważenie przez projektodawcę, czy jest to rozwiązanie właściwe. Organ do spraw ochrony danych osobowych postulował jednocześnie o uregulowanie w sposób ompleksowy, w tym w zakresie gromadzenia i archiwizacji dokumentacji w przepisach rangi ustawy, procesu rekrutacji do danego publicznego przedszkola, oddziału przedszkolnego w publicznej szkole podstawowej, publicznej innej formy wychowania przedszkolnego, publicznej szkoły, publicznej placówki, na zajęcia w publicznej placówce oświatowo-wychowawczej, na kształcenie ustawiczne w formach pozaszkolnych lub na kwalifikacyjny kurs zawodowy.

Kolejnym aspektem, na jaki GIODO zwrócił uwagę, to kwestia podawania do publicznej wiadomości wyników postępowania rekrutacyjnego, poprzez wywieszenie listy imion i nazwisk kandydatów oraz informacji o zakwalifikowaniu albo niezakwalifikowaniu kandydatów do danego publicznego przedszkola, oddziału przedszkolnego w publicznej szkoły podstawowej, publicznej innej formy wychowania przedszkolnego, publicznej szkoły, publicznej placówki, na zajęcia w publicznej placówce oświatowo-wychowawczej, na kształcenie ustawiczne w formach pozaszkolnych lub na kwalifikacyjny kurs zawodowy. Odnosząc się do projektowanej regulacji, Generalny Inspektor Ochrony Danych Osobowych odwołał się do sygnałów, które wpływają do Biura GIODO i wskazał, że wątpliwości budzi okres

retencji udostępniania tychże danych, jak i sposób podawania do wiadomości publicznej. Znane są GIODO przypadki udostępniania danych w zakresie szerszym niż przewidują to przepisy prawa, w tym w sieci Internet[128]. GIODO zasugerował, aby w ustawie wskazać okres udostępnienia tych danych na potrzeby informowania o wynikach rekrutacji. Wskazany czas przechowywania danych może być zróżnicowany w zależności od spodziewanego terminu ich użyteczności, tak aby po jego upływie, wobec braku szczególnych okoliczności, dane te były usuwane. W związku z powyższym projektodawca powinien wskazać w ustawie również okres, przez jaki przedmiotowa lista może być podawana do wiadomości publicznej.

GIODO zwrócił również uwagę, iż projekt nie zwiera regulacji, w jaki sposób wskazywane mają być osoby prawne lub fizyczne prowadzące szkołę lub placówkę w zaświadczeniu o wpis do ewidencji. Zakres wymaganych danych osobowych powinien być adekwatny do celu ich przetwarzania, w związku z czym projektodawca powinien wprost określić w przepisach ustawy, w jaki sposób osoba prawna lub osoba fizyczna ma zostać wskazana w ww. zaświadczeniu o wpisie do ewidencji.

W piśmie z dnia 27 października 2016 r.[129] Minister Edukacji Narodowej odniósł się do uwag wniesionych do projektu przez Generalnego Inspektora Ochrony Danych Osobowych. Ustawa została podpisana przez Prezydenta RP 9 stycznia 2017 r.

SKŁADKA AUDIOWIZUALNA POD LUPĄ GIODO

W opisywanym okresie sprawozdawczym GIODO wypowiedział się również na temat poselskiego projektu ustawy o składce audiowizualnej[130]. Nie negując koncepcji zastąpienia systemu opłat abonamentowych systemem składki audiowizualnej, ani wybranego wariantu poboru składki, tj. powiązania go z poborem opłat za energię elektryczną, Generalny Inspektor wskazał, iż projektowane przepisy wymagają szczegółowej analizy pod kątem ich zgodności z regulacjami dotyczącymi ochrony danych osobowych. Miało to szczególne znaczenie wobec okoliczności, iż w związku z realizacją zadań wynikających z projektu ustawy **miałoby dochodzić do przetwarzania danych osobowych (w tym również tzw. danych szczególnie chronionych) szerokiego kręgu osób (odbiorców końcowych) przez różne podmioty (inkasentów, organy gminy, organy podatkowe).** Dlatego, w celu uniknięcia wątpliwości i zapewnienia sprawnej realizacji projektowanych rozwiązań w praktyce, konieczne było, aby już na etapie formułowania przepisów określone zostały role poszczególnych podmiotów oraz zakres danych osobowych, do których podmioty te mają dostęp.

W odniesieniu do opiniowanej regulacji kluczowe znaczenie miała okoliczność, iż podmioty prywatne – przedsiębiorstwa energetyczne, miały zostać włączone w realizację zadań o charakterze publicznym. Z punktu widzenia przepisów o ochronie danych osobowych istotne było, aby takie rozszerzenie kompetencji nie wiązało się jednocześnie z posze-

[128] Ustawa o ochronie danych osobowych nakłada obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których one dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania – tj. zgodnie z zasadą ograniczenia czasowego (art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych).
[129] Sygn:DPPI-WPPiP.400.12.2016.JS.
[130] DOLiS-033-145/16.

rzeniem zakresu danych osobowych dotychczas przetwarzanych przez przedsiębiorstwa energetyczne (inkasentów).

Doprecyzowania wymagało zatem, **jakie konkretnie informacje na temat odbiorców końcowych miałyby być zawarte w prowadzonej przez inkasenta ewidencji wpłat** dokonywanych tytułem składki oraz przekazywane organowi podatkowemu przez inkasenta. Dopuszczając możliwość dookreślenia tej kwestii na poziomie aktu wykonawczego (w sytuacji, gdy nie dochodzi do przetwarzania tzw. danych szczególnie chronionych, czyli danych, o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych), Generalny Inspektor Ochrony Danych Osobowych podkreślił, iż zakres przetwarzanych danych musi z przepisów wynikać w sposób jednoznaczny i powinien być uregulowany w formie katalogu zamkniętego. Powyższą uwagę należało również odnieść do kwestii informowania przez organ gminy organu podatkowego o dokonanych zgłoszeniach będących podstawą zwolnienia z obowiązku zapłaty składki oraz o zawiadomieniach dokonywanych w przypadku zmiany danych objętych zgłoszeniem. W opinii Generalnego Inspektora Ochrony Danych Osobowych nie zachodziła potrzeba, by przekazywane informacje obejmowały również przyczynę zwolnienia konkretnej osoby (odbiorcy końcowego) z obowiązku zapłaty składki – zwłaszcza, że mogłoby się to wiązać z ujawnieniem organowi podatkowemu informacji mających charakter tzw. danych szczególnie chronionych (wrażliwych), jak np. dane na temat niepełnosprawności.

Podkreślenia wymagała konieczność ustalenia ról poszczególnych podmiotów w odniesieniu do przetwarzania danych osobowych, co wiąże się także z koniecznością właściwego i precyzyjnego wyznaczenia celów, jakie poszczególne podmioty mają realizować w procesie poboru składki audiowizualnej, jak również aby wynikało to w sposób wyraźny z przepisów prawa.

Ostatecznie zrezygnowano z pomysłu wprowadzenia składki audiowizualnej w opisywanej formie.

OCENA ZDOLNOŚCI KREDYTOWEJ KONSUMENTA

Generalny Inspektor Ochrony Danych Osobowych przedstawił również swoje uwagi do projektu ustawy o kredycie hipotecznym[131].

Z perspektywy ochrony danych osobowych najbardziej istotną kwestią wymagającą odpowiedniego uregulowania w przepisach ustawy była ocena zdolności kredytowej konsumenta. Generalny Inspektor podkreślił, iż rozumie potrzebę dokonania takiej weryfikacji dla zapewnienia bezpieczeństwa finansowego oraz potrzebę wykorzystywania w tym celu danych osobowych pochodzących z różnych zbiorów, jednak należy pamiętać, iż musi się ono odbywać z poszanowaniem zasad ochrony danych osobowych, wynikających zarówno z przepisów krajowych, jak i europejskich. O ile w przypadku banków i innych instytucji ustawowo upoważnionych do udzielania kredytów hipotecznych istnieją przepisy regulujące ich działalność oraz dające gwarancje postępowania w prawnie wyznaczonych ramach, o tyle **szerokie ujęcie pojęcia „kredytodawcy" stwarzało ryzyko większej swobody przetwarzania danych osobowych przez inne podmioty udzielające kredytów hipotecznych. Z** ostrożności organ do spraw ochrony danych osobowych wskazał zatem, iż nie powinna mieć miejsca sytuacja, gdy

[131] DOLiS-033-214/16.

z uwagi na brak odpowiednich regulacji kredytodawcy niebędący bankami albo innymi instytucjami ustawowo upoważnionymi do udzielania kredytów hipotecznych w praktyce dysponowaliby szerszymi uprawnieniami w zakresie przetwarzania danych osobowych konsumentów, niż przewidziane dla banków i innych instytucji ustawowo upoważnionych do udzielania kredytów na podstawie dotychczas obowiązujących przepisów.

Odnosząc się do szczegółowych kwestii w zakresie uregulowań dotyczących oceny zdolności kredytowej, **Generalny Inspektor zwrócił uwagę na potrzebę wyjaśnienia mocą przepisów opiniowanego aktu prawnego pojęć „zbiorów danych kredytodawcy" oraz „systemów informatycznych". Z** perspektywy ochrony danych osobowych ważne jest, by było jasne z jakich zbiorów pozyskiwane są dane podlegające analizie przy ocenianiu zdolności kredytowej oraz czy wykorzystywane w tym celu systemy informatyczne są właściwie zabezpieczone.

Po przedstawieniu kolejnej wersji projektu, Generalny Inspektor Ochrony Danych Osobowych pozytywnie ocenił rozwiązanie zaproponowane w projektowanym art. 21 ust. 4, zgodnie z którym ocena zdolności kredytowej miałaby być dokonywana zgodnie z art. 70 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe oraz innymi regulacjami obowiązującymi kredytodawców. GIODO pozytywnie odniósł się również do zawężenia definicji „kredytodawcy" zawartej w art. 4 pkt 3 projektu. Zmiany te zniwelowały wątpliwości Generalnego Inspektora wyrażone wobec pierwszej wersji projektu.

Ustawa została podpisana przez Prezydenta RP 12 kwietnia 2017 r.

REJESTR W SPRAWACH WYKONYWANIA PRACY PRZEZ CUDOZIEMCÓW NA TERYTORIUM RP

Do projektu ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy[132], Generalny Inspektor Ochrony Danych Osobowych zgłosił następujące uwagi.

Projekt przewidywał prowadzenie w systemie informatycznym przez wojewodów, powiatowe urzędy pracy i ministra właściwego do spraw pracy rejestrów w sprawach wykonywania pracy przez cudzoziemców na terytorium Rzeczypospolitej Polskiej. 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 (mimo, iż w rejestrach miałyby być gromadzone dane osobowe).**

W uzasadnieniu do projektu jako cel nowelizacji wskazano wdrożenie do polskiego porządku prawnego dyrektywy 2014/36/UE[133]. GIODO zauważył, iż implementowane przepisy nie nakładają jednak na Polskę jako państwo członkowskie UE konieczności utworzenia takich rejestrów. Podejmowanie przez cudzoziemców pracy na terytorium Rzeczypospolitej Polskiej nie powinno wiązać się ze zwiększeniem uprawnień nadzorczych wobec tych osób i odbywać się kosztem ich prawa do prywatności. Przyjęcie proponowanego rozwiązania wiązało się dodatkowo z ryzykiem dyskryminacji.

Ponadto, **projekt nie regulował** zasadniczych kwestii dotyczących prowadzenia rejestru, w szczególności zaś: **katalogu danych znajdujących się w rejestrze, okresu przechowywania tych danych, zasad udostępniania**

[132] DOLiS-033-148/16.

[133] Dyrektywa Parlamentu Europejskiego i Rady 2014/36/UE z dnia 26 lutego 2014 r. W sprawie warunków wjazdu i pobytu obywateli państw trzecich w celu zatrudnienia w charakterze pracownika sezonowego.

informacji z rejestru, kręgu podmiotów mających dostęp do danych.

Pojawiła się także wątpliwość dotycząca sposobu zasilania rejestru centralnego oraz zakresu i formy przekazywanych danych – kwestią wymagającą doprecyzowania było przede wszystkim to, z jaką częstotliwością dane miałyby być przekazywane do centralnego rejestru i w jaki sposób aktualizowane, a także w jakiej formie dokonywane będą sprostowania nieprawdziwych informacji.

Ponadto w opinii Generalnego Inspektora rozważenia wymagało, na ile niezbędna jest konstrukcja zezwalająca na udostępnianie innym podmiotom zgromadzonych w rejestrze centralnym informacji.

Po dalszych konsultacjach udało się wypracować satysfakcjonujący GIODO kształt projektu. Projektodawca określił jak długo będą przetwarzane dane zgromadzone w rejestrach. Wyjaśnił również, że informacje będą wprowadzane do rejestrów przez upoważnionych pracowników urzędów obsługujących organy prowadzące rejestry, a następnie na bieżąco importowane do rejestru centralnego. Tak więc starostowie, wojewodowie i minister właściwy do spraw pracy będą odpowiedzialni za jakość wprowadzanych danych, z zastrzeżeniem swojej właściwości. Będą też obowiązani do ich poprawienia, jeżeli stwierdzona zostanie nieścisłość. Dnia 20 kwietnia 2017 r. projekt skierowano do I czytania na posiedzeniu Sejmu.

STATUS MINISTRA ZDROWIA W ODNIESIENIU DO DANYCH GROMADZONYCH w REJESTRACH MEDYCZNYCH

W opisywanym okresie sprawozdawczym nowelizowana była również ustawa o systemie informacji w ochronie zdrowia[134].

Wątpliwości Generalnego Inspektora wzbudziło proponowane rozwiązanie, które zobowiązywałoby podmiot prowadzący rejestr do przekazywania ministrowi właściwemu do spraw zdrowia, na jego wniosek, danych zawartych w rejestrze, w terminie i w sposób wskazany przez tego ministra. Projektowany przepis nie precyzował jednak, w jakich sytuacjach takie przekazywanie miałoby mieć miejsce i dla realizacji jakiego celu dane miałyby być ministrowi przekazywane. Również uzasadnienie do projektu ustawy nie określało, jakie jest *ratio legis* wprowadzenia tego przepisu.

Konsekwencją proponowanej zmiany była utrata przez ministra właściwego do spraw zdrowia statusu administratora danych gromadzonych w rejestrach medycznych, a co za tym idzie – utrata swobodnego dostępu do tych danych oraz prawa do decydowania o celach i środkach przetwarzania danych. Dlatego konieczne było dokonanie oceny, czy wprowadzenie takiego rozwiązania jest rzeczywiście niezbędne i należycie uzasadnione, a jeżeli tak – istniała potrzeba odpowiedniego doprecyzowania przepisów w tym zakresie.

Ponadto uzasadnione było odniesienie również do ministra właściwego do spraw zdrowia tak, aby również był on zobowiązany do stworzenia warunków organizacyjnych i technicznych zapewniających ochronę przekazanych mu danych przed nieuprawnionym dostępem,

[134] DOLiS-033-378/16.

nielegalnym ujawnieniem lub pozyskaniem, a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą.

W kolejnej wersji projektu zaproponowano dalej idące zmiany związane z kwestiami przetwarzania danych osobowych, do których GIODO również zgłosił liczne uwagi.

Generalny Inspektor wskazał m.in., iż konsekwencją możliwości wymiany danych osobowych między rejestrami może być stan, w którym do poszczególnych rejestrów będą trafiać dane w zakresie szerszym, niż zezwalają na to przepisy wykonawcze, co byłoby sprzeczne z zasadą legalizmu, wyrażoną w art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych. Mimo iż ogólne cele tworzenia rejestrów medycznych są wspólne, należy zauważyć, że każdy z rejestrów dedykowany jest określonej kwestii, zatem szczegółowe cele ich prowadzenia są odmienne, ograniczone zakresem przetwarzanych danych. W**ymiana danych między rejestrami medycznymi mogłaby skutkować naruszeniem wyżej zasady celowości, jako że w efekcie dochodziłoby do zmiany pierwotnego celu przetwarzania danych**. Rozumiejąc, iż pozyskiwanie danych z innych rejestrów może być w pewnych sytuacjach uzasadnione, Generalny Inspektor wskazał, iż nie może być to dostęp o charakterze stałym, a ograniczony wyłącznie do możliwości pozyskiwania danych w indywidualnych przypadkach i w określonym w przepisach celu.

Wątpliwości Generalnego Inspektora Ochrony Danych Osobowych wzbudziło także rozwiązanie w zakresie monitorowania zapotrzebowania na świadczenia opieki zdrowotnej, monitorowania jakości i efektywności kosztowej badań lub procedur medycznych oraz prowadzenia profilaktyki zdrowotnej. Zdaniem GIODO, zbędne dla realizacji tego celu jest dysponowanie przez Narodowy Fundusz Zdrowia danymi osobowymi o charakterze jednostkowym. Konieczne było zatem dokonanie oceny, czy wprowadzenie rozwiązania, o którym była mowa, rzeczywiście są niezbędne i należycie uzasadnione i czy dla realizacji określonych w tym przepisie celów nie byłoby wystarczające pozyskiwanie danych pozbawionych charakteru zindywidualizowanego – podobnie jak ma się to odbywać w przypadku przekazywania danych z rejestrów medycznych ministrowi właściwemu do spraw zdrowia.

Odnosząc się zaś do proponowanych zmian w przepisach ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, stwierdzić należało, iż wymagają one dalszego doprecyzowania. Dodanie nowego przepisu, zgodnie z którym prezes Narodowego Funduszu Zdrowia jest obowiązany do prowadzenia i utrzymywania elektronicznego systemu monitorowania programów zdrowotnych sugerowało, iż zostanie stworzony nowy rejestr danych osobowych. Tymczasem nie jest jasne, jaki miałby być sposób zasilania takiego rejestru – a tym samym z jakich źródeł, w jakiej formie oraz w jakim trybie Fundusz pozyskiwałby dane niezbędne dla realizacji określonych w przepisach celów.

Ze względu na konieczność ochrony praw osób, których dane dotyczą oraz zagwarantowania wysokiego poziomu bezpieczeństwa danych szczególnie chronionych, Generalny Inspektor Ochrony Danych Osobowych opowiedział się za utrzymaniem zakazu dalszego powierzania przetwarzania danych zawartych w rejestrach medycznych (tzw. podpowierzania). Nie było dopuszczalne przyjęcie zaproponowanej przez projektodawcę konstrukcji, zgodnie z którą dla „podpowierzenia" przetwarzania danych wystarczające byłoby jedynie uzyskanie pisemnego upoważnienia administratora danych, gdyż takie rozwiązanie

w praktyce pozbawiłoby administratora realnego wpływu na organizację procesu przetwarzania danych. Dalsze powierzanie przetwarzania danych zawartych w rejestrach medycznych innym podmiotom wyspecjalizowanym w utrzymywaniu infrastruktury techniczno-systemowej i zapewnianiu obsługi technicznej systemów teleinformatycznych nie mogłoby również prowadzić do osłabienia poziomu bezpieczeństwa tych danych, które – jako tzw. dane wrażliwe – podlegają szczególnemu reżimowi ochrony zgodnie z art. 27 ustawy o ochronie danych osobowych.

Uwagi GIODO zostały uwzględnione przez projektodawcę, jednak prace nad projektem do tej pory nie zostały zakończone.

NOWY REJESTR KARNY – PRZESTĘPSTWA NA TLE SEKSUALNYM

Odnosząc się do projektu ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym[135], **Generalny Inspektor zwrócił uwagę na nieprzeprowadzenie uzgodnień międzyresortowych oraz konsultacji publicznych nad tak ważnym z punktu widzenia opinii publicznej dokumentem**. GIODO przestrzegł, że proponowana regulacja wchodzi w zakres prawa do prywatności oraz prawa do ochrony danych osobowych ujętych odpowiednio w art. 47 i 51 Konstytucji RP i jako taka jest w polskim porządku prawnym dopuszczalna zgodnie z art. 31 ust. 3 Konstytucji RP jedynie pod pewnymi warunkami. Organ zgłosił zastrzeżenia do tworzenia nowego rejestru karnego, gdy istnieje i z powodzeniem funkcjonuje Krajowy Rejestr Karny. **GIODO sprzeciwił się upublicznianiu informacji o imionach rodziców, nazwisku rodowym matki, numerze PESEL oraz adresie zameldowania i zamieszkania skazanego**. Zaznaczył, iż po wejściu w życie przedmiotowych przepisów Polska może spodziewać się wnoszenia spraw przed sądy polskie i międzynarodowe w związku z nieproporcjonalnym naruszeniem prawa do prywatności oraz ochrony danych osobowych przez osoby ujęte w rejestrze. Opinie Generalnego Inspektora oraz innych podmiotów dołączone do dokumentacji przebiegu sejmowego procesu legislacyjnego zawierały streszczenie najważniejszych wyroków zapadających w sprawie podobnych rejestrów w państwach europejskich oraz funkcjonowania takich baz danych w innych państwach świata. Ustawa została uchwalona i weszła w życie 1 października 2017 r.

OCHRONA DANYCH OOBSOWYCH NAUCZYCIELI UKARANYCH KARĄ DYSCYPLINARNĄ

Opiniując projekt ustawy o zmianie ustawy – Karta Nauczyciela oraz o zmianie niektórych innych ustaw[136] **GIODO zgłosił zastrzeżenie wobec zamieszczania w centralnym rejestrze orzeczeń dyscyplinarnych** wobec nauczycieli **nazwiska rodowego** nauczyciela prawomocnie ukaranego karą dyscyplinarną zwolnienia z pracy z zakazem przyjmowania ukaranego do pracy w zawodzie nauczycielskim w okresie 3 lat od ukarania albo karą dyscyplinarną wydalenia z zawodu nauczycielskiego, albo nauczyciela zawieszonego w pełnieniu obowiązków.

W opinii Generalnego Inspektora Ochrony Danych Osobowych przewidziany w ustawie – Karta Nauczyciela katalog „danych identyfikujących nauczyciela" jest wystarczający dla jednoznacznego wskazania

[135] DOLiS-033-23/16.
[136] DOLiS-033-7/16.

osoby ukaranej albo zawieszonej w pełnieniu obowiązków także bez informacji o nazwisku rodowym tej osoby, a zatem dana (informacja) o nazwisku rodowym nauczyciela jest daną zbędną. Zgodnie zaś z zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane, dane zbędne (nieadekwatne) nie powinny być gromadzone.

Za prawidłowością tego stanowiska organu do spraw ochrony danych osobowych przemawiała dodatkowo okoliczność, iż inne rejestry osób ukaranych dyscyplinarnie nie przewidują zbierania informacji o nazwisku rodowym ukaranego (ukaranej).

Jako przykład rejestrów zawierających dane osób ukaranych za przewinienia dyscyplinarne, a niezawierających ich nazwisk rodowych wspomnieć w tym miejscu należy o rejestrze Ukaranych Lekarzy i Lekarzy Dentystów Rzeczypospolitej Polskiej – art. 110 ustawy z dnia 2 grudnia 2009 roku o izbach lekarskich[137] oraz rejestrze ukaranych pielęgniarek i położnych – art. 85 ustawy z dnia 1 lipca 2011 roku o samorządzie pielęgniarek i położnych[138].

W uchwalonej przez Parlament i podpisanej przez Prezydenta Rzeczypospolitej Polskiej ustawie z dnia 18 marca 2016 roku o zmianie ustawy – Karta Nauczyciela oraz o zmianie niektórych innych ustaw[139] uwagi Generalnego Inspektora Ochrony Danych Osobowych zostały uwzględnione, centralny rejestr orzeczeń dyscyplinarnych nie zawiera nazwiska rodowego nauczyciela prawomocnie ukaranego karą dyscyplinarną zwolnienia z pracy z zakazem przyjmowania ukaranego do pracy w zawodzie nauczyciela w okresie 3 lat od ukarania albo karą dyscyplinarną wydalenia z zawodu nauczyciela, albo nauczyciela zawieszonego w pełnieniu obowiązków.

IPN WYŁĄCZONY SPOD STOSOWANIA PRZEPISÓW O OCHRONIE DANYCH

Nie tak dużym sukcesem jak w poprzednim przypadku zakończyły się prace legislacyjne w odniesieniu do projektu ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw[140].

W pierwszej kolejności Generalny Inspektor Ochrony Danych Osobowych zarzucił, że zaproponowane unormowania dotyczące przechowywania materiału genetycznego i wykorzystywania wyników badań genetycznych krewnych osób, które straciły życie wskutek walki z narzuconym systemem totalitarnym lub wskutek represji totalitarnych lub czystek etnicznych od dnia 8 listopada 1917 roku do dnia 31 lipca 1990 roku, są niewystarczające. Zagadnieniu temu poświęcony został bowiem zaledwie jeden przepis ustawy, zaś znaczna część tej problematyki miała zostać przekazana do uregulowania w akcie wykonawczym mającym być wydanym na podstawie delegacji zawartej w projekcie przepisów. Takiej konstrukcji kwestionowanych przepisów ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, organ do spraw ochrony danych osobowych nie mógł zaakceptować w sytuacji, gdy dotyczyły one przetwarzania danych genetycznych będących danymi szczególnie chronionymi w rozumieniu art. 27 ust. 1 ustawy o ochronie danych osobowych. Zgodnie bowiem

[137] Dz. U. z 2016 r. poz. 522, z późn. zm.
[138] Dz. U. z 2011 r. Nr 174, poz. 1038, z późn. zm.
[139] Dz. U. z 2016 r. poz. 668.
[140] DOLiS-033-85/16.

z ustawą o ochronie danych osobowych – przetwarzanie danych szczególnie chronionych wymaga przepisu szczególnego rangi ustawowej, stwarzającego przy tym pełne gwarancje ochrony takich danych. Nie mogąc zatem zanegować dopuszczalności zaproponowanego rozwiązania, w myśl którego to osoby, które chcą, by ich materiał genetyczny znalazł się w, prowadzonej przez Instytut Pamięci Narodowej – Komisję Ścigania Zbrodni przeciwko Narodowi Polskiemu, Bazie Materiału Genetycznego, same przekazują swój materiał genetyczny wraz z wnioskiem o zarejestrowanie w tej bazie ich danych, Generalny Inspektor Ochrony Danych Osobowych podniósł, iż w nowelizowanych przepisach ustawy o IPN pominięto takie kwestie jak: możliwość cofnięcia przez osobę, której materiał genetyczny i dane znalazły się w Bazie Materiału Genetycznego, wniosku i skutki takiego cofnięcia[141], okres przechowywania materiału genetycznego i danych osób żyjących w Bazie Materiału Genetycznego, przesłanki usunięcia materiału genetycznego i danych osób żyjących z Bazy Materiału Genetycznego. Wszystkie te kwestie nie mogą być przekazane do unormowania w rozporządzeniu ze względu na ich podstawowy charakter dla procesu przetwarzania danych.

Oprócz tego organ do spraw ochrony danych osobowych zdecydował się ponownie[142] przedstawić problem art. 71 ustawy o IPN, który to przepis wyłącza stosowanie przepisów ustawy o ochronie danych osobowych w odniesieniu do działalności IPN, określonej w art. 1 ustawy o IPN.

W ocenie Generalnego Inspektora Ochrony Danych Osobowych takie całościowe wyłączenie stosowania unormowań o ochronie danych osobowych jest niezgodne zarówno z Konstytucją Rzeczypospolitej Polskiej, jak i traktatami europejskimi. Co więcej – podobnego wyłączenia nie przewidują ustawodawstwa innych państw należących do Europejskiego Obszaru Gospodarczego, w tym również tych spośród nich, które w swoich krajowych porządkach prawnych przewidują istnienie specjalnych instytucji powołanych do zbierania, opracowywania i ujawniania dokumentów służb specjalnych wytworzonych w okresie trwania w tych państwach ustroju totalitarnego.

Organ do spraw ochrony danych osobowych w opinii do projektu ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw wskazywał, że ochrona danych osobowych znajduje silne oparcie w przepisach prawa pierwotnego Unii Europejskiej, a prawo do ochrony danych osobowych jest statuowane zarówno w art. 8 ust. 1 Karty Praw Podstawowych Unii Europejskiej załączonej do Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzonego w Lizbonie dnia 13 grudnia 2007 r.[143], jak i w art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (Dz. U. z 2004 r. Nr 90, poz. 864/2, z późn. zm.)[144], oraz – w świetle art. 51 Konstytucji Rzeczypospolitej Polskiej – stanowi też jedno z gwarantowanych praw osobistych.

[141]Możliwość odwołania zgody na przetwarzanie danych wprost przewiduje art. 7 pkt 5 in fine ustawy o ochronie danych osobowych.

[142]Poprzednio w – skierowanym do Pani Małgorzaty Kidawy-Błońskiej – ówczesnej Marszałek Sejmu – wystąpieniu Generalnego Inspektora Ochrony Danych Osobowych na podstawie art. 19 a ust. 2 ustawy o ochronie danych osobowych z dnia 14 lipca 2015 roku o sygn. DOLiS-035-2342/15/62169, 62465, 62481.

[143] Dz. U. z 2009 r. Nr 203, poz. 1569.

[144] Dz. U. z 2004 r. Nr 90, poz. 864/2, z późn. zm.

Podniósł także, iż dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[145], przewiduje jedynie możliwość ograniczenia – w określonych sytuacjach – stosowania jej postanowień, lecz nie zezwala na całkowite wyłączenie ich stosowania. Tak więc przyjęta w obowiązującym art. 71 ustawy o IPN koncepcja zupełnego wyeliminowania stosowania wobec IPN przepisów ustawy o ochronie danych osobowych rodzić może zarzut instytucji europejskich, że Rzeczpospolita Polska – wbrew istniejącemu obowiązkowi – nie spełnia europejskich wymagań w zakresie ochrony danych osobowych.

GIODO zauważył również, że kwestionowany art. 71 ustawy o IPN skutkuje niestosowaniem w działalności IPN – zawartych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – unormowań dotyczących zabezpieczeń technicznych zbiorów danych osobowych, zaś ustawa o IPN nie ustanawia własnych regulacji odnoszących się do zabezpieczenia zbiorów danych osobowych przetwarzanych przez IPN[146].

Z tych wszystkich przyczyn Generalny Inspektor Ochrony Danych Osobowych wnosił o znowelizowanie art. 71 ustawy o IPN w ramach prowadzonych prac legislacyjnych dotyczących projektu ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw.

W uchwalonej przez Parlament i podpisanej przez Prezydenta Rzeczypospolitej Polskiej ustawie z dnia 29 kwietnia 2016 roku o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw[147] zostały uwzględnione tylko te uwagi GIODO, które dotyczyły Bazy Materiału Genetycznego. I tak, wprowadzono obowiązek dokonywania przez Prezesa IPN[148], nie rzadziej niż co dziesięć lat od ich zarejestrowania w Bazie Materiału Genetycznego, weryfikacji danych i informacji o osobach zgromadzonych w Bazie Materiału Genetycznego pod kątem celowości ich dalszego przetwarzania[149] i nałożono na Prezesa IPN powinność usunięcia z Bazy Materiału Genetycznego danych (informacji) na wniosek osób, których te dane (informacje) dotyczą[150] oraz gdy w wyniku weryfikacji stwierdzono niecelowość dalszego przetwarzania tych danych (informacji)[151].

Nie znowelizowano niestety art. 71 ustawy o IPN.

[145] Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.

[146] Zagadnienie to zostało jedynie zasygnalizowane w art. 29 ustawy o IPN, w którym zadeklarowano, iż w zakresie działalności archiwalnej IPN m.in. Zabezpiecza zgromadzoną dokumentację. Brak jest jednak przepisów precyzujących sposób dokonywania tego zabezpieczenia.

[147] Dz. U. z 2016 r. poz. 749.

[148] Administratora danych zgromadzonych w Bazie Materiału Genetycznego – art. 53 f ust. 1 ustawy o IPN, dodany przez art. 1 pkt 27 ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw.

[149] Art. 53 f ust. 4 ustawy o IPN, dodany przez art. 1 pkt 27 ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw.

[150] Art. 53 f ust. 5 zdanie pierwsze ustawy o IPN, dodany przez art. 1 pkt 27 ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw.

[151] Art. 53 f ust. 6 ustawy o IPN, dodany przez art. 1 pkt 27 ustawy o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz o zmianie niektórych innych ustaw.

ZMIANY W KPA

Istotne wątpliwości organu do spraw ochrony danych osobowych wzbudził – zawierający wiele nowatorskich rozwiązań prawnych – projekt ustawy o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw[152]. W swoim stanowisku do tego projektu **Generalny Inspektor Ochrony Danych Osobowych podniósł m.in., że pominięto** okoliczność, że 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[153], zwane powszechnie **„rozporządzeniem eIDAS", wprowadziło zmianę terminologii w odniesieniu do podpisów elektronicznych**. Niezasadnym jest zatem posługiwanie się pojęciem „bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego certyfikatu", w sytuacji gdy – stosowane od 1 lipca 2016 roku – rozporządzenie eIDAS posługuje się terminem: „kwalifikowany podpis elektroniczny"[154].

Co więcej, w świetle przepisów ogólnego rozporządzenia o ochronie danych oraz rozporządzenia Rady (EWG) nr 1/58 z dnia 15 kwietnia 1958 r. W sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej[155] jeden z przepisów mógł być uznany za **sprzeczny z prawem Unii Europejskiej. W**prowadzał on bowiem formalne wymaganie, zgodnie z którym **rozpatrzenie przez polski organ administracji publicznej (a więc również Generalnego Inspektora Ochrony Danych Osobowych)** wniosku organu administracji publicznej innego państwa członkowskiego Unii Europejskiej albo organu administracji Unii Europejskiej o udzielenie niezbędnej pomocy **jest uzależnione od sporządzenia wniosku o tę pomoc w języku polskim**. Tymczasem ogólnym rozporządzeniu o ochronie danych przewidującym mechanizm współpracy między polskim organem nadzorczym, Komisją Europejską, Europejską Radą Ochrony Danych oraz organami nadzorczymi innych państw członkowskich Unii Europejskiej, brak jest jakichkolwiek regulacji dotyczących języka, w którym mają być przekazywane informacje w ramach mechanizmu współpracy. Tym samym przyjąć należy, iż informacje te mogą być przekazywane w każdym z oficjalnym języków Unii Europejskiej, a zatem przepis nakładający obowiązek stosowania wyłącznie języka polskiego pozostawał w sprzeczności z unormowaniami unijnej reformy ochrony danych. Ograniczał on także – przewidziane w rozporządzeniu Rady (EWG) nr 1/58 w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej – uprawnienie instytucji unijnych do określenia szczegółowych zasad stosowania systemu językowego w swych wewnętrznych regulaminach postępowania, „wymuszając" na instytucjach unijnych kierowanie do polskich organów administracji publicznej wszelkiej korespondencji w języku polskim.

Wątpliwości organu do spraw ochrony danych osobowych budziła również dyspozycja nowego art. 104 a k.p.a., tym bardziej, że został on umiejscowiony w rozdziale zawierającym ogólne przepisy odnoszące się do decyzji administracyjnych. Rozumiejąc

[152] DOLiS-033-286/16.
[153] Dz. Urz. UE L 257 z 28.08.2014, str. 73.
[154] Art. 3 pkt 12 rozporządzenia eIDAS.
[155] Dz. Urz. Wspólnot Europejskich P 17 z 06.10.1958, str. 385, z późn. zm.

słuszne intencje Projektodawcy[156], które legły u podstaw tej regulacji, Generalny Inspektor Ochrony Danych Osobowych zauważył, iż zastosowanie komentowanego przepisu może w praktyce skutkować naruszeniem zasad postępowania administracyjnego. W sytuacji bowiem, w której w postepowaniu wszczętym na żądanie strony występuje druga strona (inne strony) o sprzecznych interesach, zastosowanie tego przepisu przez organ administracji publicznej oznaczać będzie w istocie faworyzowanie strony, na żądanie której wszczęto postępowanie[157], z pominięciem interesów strony przeciwnej (albo pozostałych stron postępowania). Strona przeciwna stronie żądającej wszczęcia postępowania (albo inne strony postępowania) może (mogą) w takich okolicznościach zasadnie uważać, że organ administracji publicznej naruszył wobec niej (nich) reguły bezstronności i równego traktowania. Dlatego, uwzględniając dodatkowo fakt, iż stosowanie art. 104 a k.p.a., wymagać będzie niekiedy dokonania przez organ administracji publicznej swoistego „przedsądu", Generalny Inspektor Ochrony Danych Osobowych wniósł o poprawienie tego przepisu.

Stosownego poprawienia wymagały również przepisy, które opatrywały formułą „w szczególności" katalogi przetwarzanych danych osobowych, czyniąc je otwartymi. Taka konstrukcja kwestionowanych przepisów skutkowałaby możliwością przetwarzania – w protokole z przebiegu mediacji, w umowie administracyjnej, w protokole z postępowania mediacyjnego – w istocie dowolnych danych osobowych, co pozostaje w sprzeczności z zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane[158]. Dlatego organ do spraw ochrony danych osobowych wnosił o wykreślenie tych przepisów.

Większość uwag Generalnego Inspektora Ochrony Danych Osobowych skutkowało wprowadzeniem zmian do projektu ustawy o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw.

NIEDOZWOLONE DUBLOWANIE PODSTAW PRAWNYCH PRZETWARZANIA DANYCH

Generalny Inspektor brał również udział w opiniowaniu rozporządzenia Ministra Edukacji Narodowej w sprawie Kolegium Arbitrażu Egzaminacyjnego[159]. Organ do spraw ochrony danych osobowych zwrócił uwagę, iż zamieszczona w projekcie klauzula zgody na przetwarzanie danych osobowych we wniosku o wpis na listę arbitrów, zgodnie z obowiązującymi przepisami prawa nie jest potrzebna. O **ile bowiem wykorzystywanie danych służy realizacji uprawnienia lub obowiązku określonego w przepisach prawa, to nie jest potrzebne dodatkowo pozyskiwanie zgody osoby na takie wykorzystywanie danych**[160].

[156] Szczegółowo wyjaśnione w uzasadnieniu projektu nowelizacji k.p.a. – str. 8–9.
[157] Ma ona de facto zostać pouczona przez organ administracji publicznej jakie fakty i dowody powołać, by uzyskać decyzję zgodną ze swoim żądaniem.
[158] Art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.
[159] DOLiS-033-325/16.
[160] Zgodnie z art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; Odbieranie zgody wówczas, gdy wykorzystywanie danych służy realizacji normy prawnej, wprowadza w błąd, a także sugeruje możliwość wyboru, podczas gdy przekazanie danych jest obowiązkiem, bez którego cel pozyskania danych nie mógłby zostać zrealizowany. Co do zasady jednak, jeśli przetwarzanie danych osobowych nie ma podstaw w przepisach prawa, wtedy zgoda osoby, której dane są przetwarzane, jest wymagana, projektodawca powinien natomiast stworzyć takie regulacje, aby wymóg

Ponadto w projekcie zastrzeżenia organu do spraw ochrony danych osobowych wzbudził wymóg obligatoryjnego podania przez wnioskodawcę: miejsca zatrudnienia, adresu do korespondencji, numeru telefonu i adresu e-mail. Wskazane we wniosku dane, tj. imię i nazwisko, stopień lub tytuł w dziedzinie nauki lub sztuki, nazwa przedmiotu, z którego przeprowadzany jest egzamin maturalny lub nazwa kwalifikacji, w zakresie której kandydat ubiega się o wpis, mają swoje uzasadnienie w szczególnych przepisach prawa[161], jednak pozostałe dane nie mają takiego uzasadnienia. Jeżeli podanie adresu do korespondencji, numeru telefonu i adresu e-mail miałoby służyć ułatwieniu kontaktu z osobą ubiegającą się o wpis na listę, konieczne byłoby zaznaczenie, iż podanie tych danych jest dobrowolne. Żądanie numeru telefonu i adresu e-mail powinno mieć charakter fakultatywny i dobrowolny, nie ma bowiem obowiązku posiadania obu tych źródeł kontaktu. Dodatkowo GIODO wskazał, iż obowiązek podania we wniosku miejsca zatrudnienia nie jest w żaden sposób uzasadniony, nie wiadomo zatem, jaki miałby być cel podawania tej informacji i jej dalszego przetwarzania.

GIODO zaznaczył także, że przepisy szczególne dotyczące arbitrów powinny wyczerpująco wyznaczać zasady przetwarzania ich danych osobowych w związku z funkcjonowaniem Kolegium, a rozwiązania przyjmowane w akcie wykonawczym nie powinny stanowić rozwiązań zastępujących przepisy ustawy, w tym w odniesieniu do zakresu przetwarzania danych osobowych.

Prace legislacyjne nad projektem nie zostały zakończone w okresie sprawozdawczym.

ZAKRES DANYCH POWINIEN BYĆ ZAWSZE ZWIĄZANY Z CELEM PRZETWARZANIA

Liczne uwagi GIODO wzbudził również artykuł dotyczący „listy rzeczoznawców". **Organ do spraw ochrony danych osobowych wskazał, iż nie zawarto w nim, jakie dane osobowe rzeczoznawców będzie zawierać owa lista** [162]. GIODO zwrócił również uwagę na konieczność dokonania analizy okresu przetwarzania danych zawartych na liście rzeczoznawców (tzw. okres retencji danych)[163]. Ustawa nakłada obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których one dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania – tj. zgodnie z zasadą ograniczenia czasowego. Należałoby wskazać w ustawie – Prawo łowieckie okres przetrzymywania tych danych. Wskazany czas przechowywania danych musi być zróżnicowany w zależności od spodziewanego terminu ich użyteczności, tak aby po jego upływie, wobec braku szczególnych okoliczności, dane te były usuwane. GIODO zaznaczył także, iż w ustawie nie zostało wskazane, czy i komu zostanie udostępniona „lista rzeczoznawców".

udostępniania określonych danych osobowych miał podstawę w przepisach prawa (zasada praworządności, legalizmu). Jeżeli zatem przetwarzanie danych osobowych osób ubiegających się o wpis na listę arbitrów, ma swoje uzasadnienie w obowiązujących przepisach prawa, określających podstawę prawną, cel i zakres przetwarzanych danych - odbieranie zgody na takie przetwarzanie nie jest prawidłowe.

[161] art. 9 ust. 7 ustawy o systemie oświaty (Dz.U. z 2015 r., poz.2156 z późn.zm.),

[162] powinna zawierać katalog danych zgodny z zasadą adekwatności z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

[163] Ustawa nakłada obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których one dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania – tj. zgodnie z zasadą ograniczenia czasowego, o której mowa w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych.

Wniesione przez GIODO uwagi zostały częściowo uwzględnione. Pismem z 12 kwietnia 2016 r. skierowanym do Przewodniczących Komisji Rolnictwa i Rozwoju Wsi oraz Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa[164] oraz do Sejmu[165], GIODO przyjął z zadowoleniem fakt określenia w ustawie - Prawo łowieckie katalogu danych zamieszczanych w protokole oględzin i oszacowania szkód, zwrócił jednak uwagę na dodane do omawianego zapisu sformułowania „w szczególności". GIODO wskazał, iż sformułowanie to będzie dawało swobodę w zamieszczaniu dowolnych danych w protokole oględzin i oszacowania szkód, w związku z powyższym zasugerował jego usunięcie.

Odnosząc się do „listy rzeczoznawców" Generalny Inspektor zauważył, iż nie został wskazany zakres danych osobowych rzeczoznawców, które miałaby zawierać taka lista. Biorąc pod uwagę, iż – najprawdopodobniej lista ta będzie jawna i powszechnie dostępna, udostępnione dane osobowe rzeczoznawców nie mogą zawierać danych tzw. wrażliwych. Dodatkowo GIODO wskazał, iż jeżeli projektodawca podtrzymuje zamiar zapewnienia jawności i powszechnej dostępności listy rzeczoznawców, powinien w którymś z przepisów merytorycznych dotyczących listy rzeczoznawców wprost zadeklarować tę zasadę.

Projekt ustawy został skierowany do Sejmu15 listopada 2016 r., a po pierwszym czytaniu w Sejmie przekazano go do Komisji Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa. Prace nad projektem w tej Komisji trwają do chwili obecnej.

POLSKA SŁUŻBA GEOLOGICZNA A OCHRONA DANYCH

Generalny Inspektor Ochrony Danych Osobowych przedstawił również swoje uwagi do projektu ustawy o Polskiej Służbie Geologicznej [166].

W pierwszej kolejności organ wskazał, iż **przepisy projektu nie określają w jaki sposób będzie weryfikowane spełnianie przez Prezesa Polskiej Służby Geologicznej i Strażników Straży wymogu posiadania nieposzlakowanej opinii.** Jest to kwestia bardzo istotna z punktu widzenia praw tych osób, gdyż „cieszenie się nieposzlakowaną opinią" jest jednym z wymagań, od spełnienia którego uzależniona jest możliwość sprawowania funkcji Prezesa Polskiej Służby Geologicznej albo pełnienia służby jako Strażnik Straży.

GIODO odniósł się również do zapisów, które miałyby regulować kwestię podawania do publicznej wiadomości jako informacji publicznej „informacji o wyniku postępowania". Wątpliwości organu do spraw ochrony danych osobowych wzbudziły następujące kwestie. Po pierwsze – jakie informacje Projektodawca uważa za „wynik postępowania kwalifikacyjnego" tzn. jakie dane osób biorących udział w postępowaniu kwalifikacyjnym znajdą się w tym „wyniku". Jeżeli w informacja o wyniku miałaby zawierać imię i nazwisko osoby objętej postępowaniem kwalifikacyjnym, to Generalny Inspektor wskazał, iż ustawa o ochronie danych osobowych nakłada obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których one dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania – tj. zgodnie z zasadą ograniczenia czasowego (art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych). Należałoby

[164] Sygnatura DOLIS-33-30/16/28717.
[165] Sygnatura DOLiS-33-30/16/28705.
[166] DOLiS-033-428/16.

zatem w projekcie wskazać okres udostępnienia jako informacji publicznej danych osoby objętej postępowaniem kwalifikacyjnym. Wskazany czas przechowywania danych może być zróżnicowany w zależności od spodziewanego terminu ich użyteczności, tak aby po jego upływie, wobec braku szczególnych okoliczności, dane te były usuwane. Zarówno zakres informacji podlegających upublicznieniu, jak i okres upublicznienia tych informacji na stronie internetowej Biura Polskiej Służbie Geologicznej, powinny być określone – w opinii GIODO – w ustawie, nie zaś w rozporządzeniu. Gdyby zatem w ramach upubliczniania informacji o „wyniku postępowania kwalifikacyjnego" miały być przetwarzane dane szczególnie chronione osób objętych postępowaniem kwalifikacyjnym, to tym bardziej wymagałoby to regulacji ustawowej, nie zaś wynikającej z rozporządzenia wykonawczego.

Jednocześnie organowi do spraw ochrony danych osobowych wątpliwa wydała się propozycja, by do przetwarzania danych przez PSG ustawa o ochronie danych osobowych stosowała się jedynie odpowiednio. Przyjmowanie takich rozwiązań GIODO uznaje za wysoce dyskusyjne, gdyż nie wydaje się, by przetwarzanie danych przez PSG miało charakter na tyle atypowy, aby wymagało stosowania przepisów ustawy o ochronie danych osobowych jedynie odpowiednio, a nie wprost. Co więcej – na podstawie przepisów projektu nie można w sposób jednoznaczny ustalić, jak to „odpowiednie" stosowanie przepisów ustawy o ochronie danych osobowych do przetwarzania danych przez PSG miałoby się odbywać.

Prace nad projektem nie zakończyły się, projektodawca do chwili obecnej nie odniósł się do uwag zgłoszonych przez GIODO.

MONITORING WIZYJNY W IZOLATKACH

Kolejnym z przedstawionych Generalnemu Inspektorowi Ochrony Danych Osobowych do zaopiniowania aktów legislacyjnych był projekt ustawy o zmianie ustawy o ochronie zdrowia psychicznego oraz niektórych innych ustaw[167]. W przedstawionych projektodawcy uwagach, Generalny Inspektor pozytywnie odniósł się do propozycji uregulowania w przepisach rangi ustawy podstawowych kwestii związanych ze stosowaniem monitoringu wizyjnego w pomieszczeniach przeznaczonych do izolacji. Generalny Inspektor zauważył jednocześnie, iż wydane na podstawie ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 2016 r. poz. 546, z późn. zm.) rozporządzenie z dnia 28 czerwca 2012 r. w sprawie sposobu stosowania i dokumentowania zastosowania przymusu bezpośredniego oraz dokonywania oceny zasadności jego zastosowania (Dz. U. z 2012 r. poz. 740) nie jest jedynym aktem wykonawczym Ministra Zdrowia, w którym regulowana jest kwestia monitorowania różnego rodzaju pomieszczeń[168]. **Generalny Inspektor Ochrony Danych Osobowych przypomniał o konieczności uregulowania w przepisach rangi ustawy podstawowych kwestii**

[167] DOLiS-033-464/16.

[168] Mowa tu o następujących regulacjach: Rozporządzenie Ministra Zdrowia z dnia 8 grudnia 2014 r. W sprawie izb wytrzeźwień i placówek wskazanych lub utworzonych przez jednostkę samorządu terytorialnego (Dz. U. z 2014 r. poz. 1850), Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2012 r. w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą (Dz. U. z 2012 r. poz. 739), Rozporządzenie Ministra Zdrowia z dnia 2 grudnia 2004 r. W sprawie wykazu zakładów psychiatrycznych i zakładów leczenia odwykowego przeznaczonych do wykonywania obserwacji oraz sposobu finansowania obserwacji, a także warunków zabezpieczenia zakładów dla osób pozbawionych wolności (Dz. U. z 2004 r. Nr 269, poz. 2679, z późn. zm.), Rozporządzenie Ministra Zdrowia z dnia 20 kwietnia 2005 r. w sprawie szczegółowych zasad kierowania, przyjmowania, przenoszenia, zwalniania i pobytu nieletnich w publicznych zakładach opieki zdrowotnej (Dz. U. z 2005 r. Nr 79, poz. 692).

związanych ze stosowaniem monitoringu wizyjnego również w przypadkach, których dotyczą pozostałe rozporządzenia. Jednocześnie Generalny Inspektor wskazał, iż taka forma zapewniania bezpieczeństwa jest co do zasady dopuszczalna, ale musi być stosowana zgodnie z obowiązującymi zasadami ochrony danych osobowych.

GIODO zasugerował również rozważenie, czy 6-miesięczny okres przechowywania zapisu z monitoringu jest rzeczywiście niezbędny i należycie uzasadniony, biorąc pod uwagę zasadę ograniczenia czasowego, o której mowa w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych.

GIODO wskazał ponadto, iż warto uzupełnić projektowane przepisy o gwarancję, zgodnie z którą obraz z kamer systemu telewizji przemysłowej, zainstalowanych w części celi mieszkalnej przeznaczonej do celów sanitarno-higienicznych oraz w łaźniach, jest przekazywany do monitorów lub urządzeń w sposób uniemożliwiający ukazywanie intymnych części ciała skazanego oraz wykonywanych przez niego intymnych czynności fizjologicznych.

Generalny Inspektor Ochrony Danych Osobowych z zadowoleniem przyjął natomiast uregulowanie w opiniowanym projekcie kwestii przetwarzania danych osobowych przez gminne komisje rozwiązywania problemów alkoholowych (art. 2 pkt 7 projektu)[169].

W art. 3 opiniowanego projektu znalazła się również propozycja zmiany ustawy o ochronie danych osobowych, polegająca na zwolnieniu z obowiązku zgłoszenia do rejestracji zbiorów administratorów danych przetwarzanych przez gminne komisje rozwiązywania problemów alkoholowych w celu realizacji zadań związanych z procedurą zobowiązania do poddania się leczeniu odwykowemu. W przedmiotowych zbiorach co do zasady przetwarzane są jednak dane szczególnie chronione (wrażliwe). Tym samym, z perspektywy organu do spraw ochrony danych osobowych, wprowadzenie do ustawy o ochronie danych osobowych zwolnienia z obowiązku rejestracji zbiorów danych przetwarzanych przez gminne komisje rozwiązywania problemów alkoholowych w celu realizacji zadań związanych z procedurą zobowiązania do poddania się leczeniu odwykowemu, mogło stanowić o obniżeniu stopnia ochrony danych przetwarzanych w tych zbiorach.

Uwagi Generalnego Inspektora zostały w większości uwzględnione przez projektodawcę. W szczególności Generalny Inspektor z zadowoleniem przyjął odstąpienie od propozycji zmiany ustawy o ochronie danych osobowych oraz wprowadzenie gwarancji analogicznej do art. 73a § 5 ustawy Kodeksy karny wykonawczy. Projekt ustawy został skierowany na Stały Komitet Rady Ministrów w kwietniu 2017 r.

DANE OSOBOWE ZMARŁEGO PACJENTA

Przedmiotem uwag GIODO był także projekt ustawy o zmianie ustawy – Kodeks postępowania karnego ustawy o zawodach lekarza i lekarza dentysty oraz ustawy o prawach pa-

[169] Zagadnienie to było przedmiotem szczególnego zainteresowania organu – w dniu 27 kwietnia 2011 r. (sprawa o sygnaturze DOLiS-035-1187/11, http://www.giodo.gov.pl/1520122/id_art/4183/j/pl/,) Generalny Inspektor skierował do Ministerstwa Zdrowia wystąpienie, w którym postulował stworzenie jasnych i rzetelnych procedur regulujących proces przetwarzania danych osobowych, w tym m. in. określenie katalogu danych przetwarzanych przez gminne komisje rozwiązywania problemów alkoholowych (korespondencja w tej sprawie była również kierowana do resortu zdrowia w dniu 12 września 2016 r.), co zostało uwzględnione w opiniowanym przez GIODO projekcie.

cjenta i Rzeczniku Praw Pacjenta (druk senacki nr 201)[170]. Nie był on przedstawiony Generalnemu Inspektorowi do zaopiniowania przez projektodawcę.

Art. 2 i 3 ustawy przewidywał zmiany w przepisach ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2015 r. poz. 464, z późn. Zm.) oraz ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2016 r. poz. 186, z późn. Zm.). Ich konsekwencją miała być możliwość wyrażenia zgody przez osobę bliską na ujawnienie tajemnicy lekarskiej po śmierci pacjenta.

Rozwiązanie to nie mogło spotkać się z akceptacją ze strony Generalnego Inspektora Ochrony Danych Osobowych. Wprawdzie ustawa o ochronie danych osobowych swoim zakresem nie obejmuje danych osób zmarłych, jednak ujawnienie tajemnicy lekarskiej nawet po śmierci pacjenta może – z uwagi na jej specyfikę – wiązać się również z ujawnieniem danych osób żyjących.

Osoby bliskie nie są z mocy prawa upoważnione do dostępu do informacji na temat stanu zdrowia pacjenta nawet za jego życia. Jak stanowi art. 31 ust. 2 ustawy o zawodach lekarza i lekarza dentysty, lekarz może udzielić informacji o stanie zdrowia pacjenta innym osobom za zgodą pacjenta lub jego przedstawiciela ustawowego. Osoby bliskie nie są zatem uprawnione do dostępu do informacji o stanie zdrowia pacjenta bez jego wyraźnej zgody. Zgodnie zaś z art. 26 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, po śmierci pacjenta, prawo wglądu w dokumentację medyczną ma osoba upoważniona przez pacjenta za życia. W związku z powyższym należało przyjąć, iż **pacjent (a w szczególnych sytuacjach jego przedstawiciel ustawowy) jest co do zasady wyłącznym dysponentem informacji na temat swojego stanu zdrowia** i może wedle swojego uznania określać krąg osób upoważnionych do zapoznania się z takimi informacjami.

Nie było zatem dopuszczalne przyjęcie rozwiązania, zgodnie z którym po śmierci pacjenta dostęp osób bliskich do informacji o jego stanie zdrowia stałby się w zasadzie nieograniczony. Zarówno za życia, jak i na wypadek śmierci, to pacjent powinien decydować o tym, kto zostanie dopuszczony do informacji objętych tajemnicą lekarską. Dane znajdujące się w dokumentacji medycznej to w wielu sytuacjach bardzo osobiste, intymne informacje, którymi pacjent może nie chcieć się dzielić z kimkolwiek, nie tylko za życia, ale także po swojej śmierci – i w dotychczasowym stanie prawnym miał taką możliwość.

Wreszcie, nie można w sposób jednoznaczny przesądzić, iż po śmierci pacjenta informacje objęte tajemnicą lekarską nie podlegają ochronie na mocy przepisów ustawy o ochronie danych osobowych. Niejednokrotnie – np. w przypadku chorób genetycznych – dane osób zmarłych dotyczyć mogą również osób żyjących i w takim przypadku w sposób pośredni (jako dane żyjącego członka rodziny) zostać objęte przepisami o ochronie danych osobowych. Nie powinna być zatem dopuszczalna sytuacja, by to decyzja innej osoby – nawet jeśli jest to osoba bliska – była podstawą udostępnienia tego rodzaju danych. Z uwagi na powyższe, Generalny Inspektor Ochrony Danych Osobowych wskazał na konieczność rezygnacji z proponowanych zmian w przepisach ustawy o zawodach lekarza i lekarza dentysty oraz ustawy o prawach

[170] DOLiS-033-218/16.

pacjenta i Rzeczniku Praw Pacjenta, jednak jego uwagi nie zostały uwzględnione.

CO POWINIEN WIEDZIEĆ POŚREDNIK NIERUCHOMOŚCI?

Wśród opiniowanych przez Generalnego Inspektora projektów aktów prawnych znalazł się również projekt ustawy o zmianie ustawy o gospodarce nieruchomościami.

Istotną kwestią wymagającą wyjaśnienia było umożliwienie pośrednikom w obrocie nieruchomościami wglądu oraz pobierania odpowiednich wpisów, wypisów i zaświadczeń zawartych w rejestrach dotyczących nieruchomości i praw do nieruchomości. Ponieważ **pośrednicy uzyskaliby w ten sposób dostęp do szerokiego zakresu danych, w tym również danych osobowych**, konieczne było dokonanie oceny, czy wprowadzenie takiego rozwiązania w proponowanym kształcie było rzeczywiście niezbędne i należycie uzasadnione. **Dotyczyło to zwłaszcza prawa dostępu do ewidencji ludności, ponieważ rejestr PESEL**, rejestry mieszkańców oraz rejestry zamieszkania cudzoziemców (w których prowadzona jest ewidencja ludności) nie są rejestrami „dotyczącymi nieruchomości i praw do nieruchomości", a zawierają obszerny katalog danych osobowych, których pozyskiwanie nie jest niezbędne dla prawidłowego wykonywania czynności przez pośrednika w obrocie nieruchomościami. Należało zatem precyzyjnie określić jakie dane z tychże rejestrów, w tym z ewidencji ludności mogą być pozyskiwane przez pośredników.

Jednocześnie należało rozważyć, czy rzeczywiście niezbędne było ogłaszanie w dzienniku urzędowym ministra właściwego do spraw budownictwa, lokalnego planowania i zagospodarowania przestrzennego oraz mieszkalnictwa oraz publikacja na stronach internetowych urzędu obsługującego ministra danych dotyczących imion rodziców osób, którym nadano uprawnienia zawodowe rzeczoznawców majątkowych. Nie był bowiem jasny cel, jakiemu miałoby to służyć, a w opinii Generalnego Inspektora pozostałe udostępniane dane były wystarczające dla identyfikacji rzeczoznawców majątkowych.

Projektodawca co do zasady pozytywnie odniósł się do powyższych uwag. GIODO z zadowoleniem przyjął zwłaszcza dookreślenie przez projektodawcę, iż dostęp do ewidencji ludności odbywa się w zakresie spełnienia obowiązku meldunkowego. Wyjaśniono ponadto, iż w centralnym rejestrze rzeczoznawców majątkowych wpisuje się wyłącznie informację o rodzaju orzeczonej kary dyscyplinarnej i nie podlega ona udostępnieniu w dzienniku urzędowym oraz na stronie internetowej. W kwietniu 2017 r. projekt został przekazany Radzie Ministrów.

ZMIANY W USTAWIE O KOMORNIKACH SĄDOWYCH

Ocenie Generalnego Inspektora został poddany przedstawiony przez Ministerstwo Sprawiedliwości projekt ustawy o komornikach sądowych[171], w którym jedna z podstawowych regulacji dotyczyła wprowadzenia przepisów umożliwiających załatwianie wielu spraw za pośrednictwem systemów teleinformatycznych. Rozwiązania tego Generalny Inspektor Ochrony Danych Osobowych nie ocenił negatywnie jako takiego, zwrócił jednak uwagę na konieczność doprecyzowania przepisów polegającą w szczególności – w kontekście

[171] DOLiS-033-563/16.

wykonywania przez Ministra Sprawiedliwości nadzoru nad komornikami – na **sprecyzowaniu celów i określenie kompetencji Ministra Sprawiedliwości związanych z przetwarzaniem danych osobowych projektowanego systemu teleinformatycznego**. To z treści przepisów powszechnie obowiązującego prawa – na wszystkich płaszczyznach działania Ministra Sprawiedliwości – jednoznacznie ma wynikać jakie są jego ustawowe kompetencje w zakresie przetwarzania danych osobowych na gruncie przepisów o komornikach sądowych. Taki postulat jest niezbędny zarówno z punktu widzenia zupełnej regulacji danej materii w akcie prawnym, ochrony danych osobowych komorników, asesorów i aplikantów komorniczych, danych osobowych uczestników postępowania egzekucyjnego, ale również uniknięcia wątpliwości interpretacyjnych choćby w przypadku realizacji uprawnień nadzorczych.

Generalny Inspektor poddał ocenie również regulację przewidującą prawo komornika do żądania za pośrednictwem środków komunikacji elektronicznej od określonych organów, banków, spółdzielczych kas, zarządów wspólnot mieszkaniowych, innych podmiotów zarządzających mieszkaniami i lokalami użytkowymi, jak również innych instytucji, informacji dotyczących stanu majątkowego dłużnika, danych adresowych oraz innych informacji umożliwiających identyfikację składników jego majątku. Projekt ustawy nie zawierał opisu procesu, w toku którego ma się odbywać kierowanie tych zapytań i jakie dane osobowe dłużnika mają być wykorzystywane na tę okoliczność. Istotnym jest również określenie zakresu danych osobowych oraz rodzajów systemów, do których są one wprowadzane, jak również informacji uzyskiwanych w wyniku takiej czynności – celem określenia zakresu przetwarzanych danych osobowych.

Organ ochrony danych osobowych zwrócił również uwagę, że nie jest jasne jakie urządzenia ewidencyjne i jakie dane, w tym dane osobowe, w nich zawarte (bądź zawarte na nośnikach danych) mają być przekazywane w ramach likwidacji kancelarii odwołanego komornika albo komornika, którego powołanie wygasło z mocy prawa przez likwidatora i prezesa właściwego sądu apelacyjnego, a także na brak opisu schematu systemu teleinformatycznego budowanego na potrzeby obsługi systemu egzekucji komorniczej oraz do wprowadzenia nadzoru nad komornikami. Projekt opiniowanej ustawy przewidywał bowiem, że dokumentacja jest prowadzona w systemie teleinformatycznym, którego administratorem jest Minister Sprawiedliwości. Pomimo przepisu, że to Minister Sprawiedliwości administruje systemem, nie sposób nie zauważyć, iż częścią systemu jest dokumentacja w nim zawarta, a administrator systemu ex definitione ma dostęp do wszystkich informacji w nim zawartych, w tym również każdego pliku znajdującego się w systemie.

W odniesieniu do aspektu utrwalania poprzez **obraz i dźwięk** przebiegu czynności egzekucyjnych dokonywanych przez komornika poza kancelarią, **Generalny Inspektor Ochrony Danych Osobowych zwrócił się z prośbą do Ministra Sprawiedliwości o rozważenie czy utrwalanie wszystkich czynności egzekucyjnych za pomocą urządzenia rejestrującego jest rzeczywiście niezbędne**, czy też powinno być ograniczone np. do określonej kategorii spraw. Przy dokonywaniu tych czynności dochodzi bowiem do pozyskania wielu danych, obrazów, czy też wizerunku osób biorących udział w czynnościach komorniczych, jak również wizerunku osób postronnych. Dochodzi zatem do ingerencji w prywatność osób objętych takim rodzajem rejestrowania. Projektodawca powinien zatem rozważyć czy w istocie takie rozwiązanie jest adekwatne

(proporcjonalne) do praw osób, których owa rejestracja dotyczy. Generalny Inspektor wskazał również na konieczność przewidzenia w przepisach powszechnie obowiązującego prawa rozwiązania polegającego na dokonywaniu cyklicznych przeglądów materiałów powstałych w wyniku dokumentowania pracy komornika, celem weryfikacji czy ich przechowywanie w aktach sprawy jest niezbędne oraz wprowadzenia obowiązku usuwania nagrań, gdy staną się już one zbędne dla postępowania egzekucyjnego. Ponadto, decydując o przyjęciu rozwiązania polegającego na utrwalaniu przebiegu czynności egzekucyjnych dokonywanych przez komornika poza kancelarią za pomocą urządzenia rejestrującego obraz i dźwięk, projektodawca powinien pamiętać, że powinno mu również towarzyszyć wprowadzenie odpowiednich zabezpieczeń technicznych uniemożliwiających dokonanie jakichkolwiek modyfikacji czy zmian w rejestrowanym materiale.

Dodać tutaj również należy, iż ani przepisy projektowanej ustawy, ani uzasadnienie projektu nie precyzowały czy system teleinformatyczny ma przetwarzać materiały pozyskane na postawie projektowanego art. 809[1] Kodeksu postępowania cywilnego, czy też utrwalony obraz i dźwięk ma być przechowywany w ramach innego systemu teleinformatycznego lub poza systemem – chodzi tu o nośniki informacji w postaci elektronicznej (np. dysk CD, taśma magnetyczna czy dysk USB). Całość powstałych w wyniku nowych rozwiązań technicznych zapisów będzie stanowiła dokumentację komorniczą objętą tajemnica komorniczą.

W odniesieniu do wprowadzanych rozwiązań teleinformatycznych Generalny Inspektor wskazał również, że projekt ustawy co prawda zawiera **termin, w jakim dokumentacja może być również tworzona, przetwarzana i przechowywana w postaci dotychczasowej**, nie zawiera on jednak sankcji, jak również ewentualnych skutków faktycznych dla komorników, którzy nie dostosują się do rozwiązań polegających na przejściu na cyfrowy obieg dokumentacji. Niezwykle ważne jest także określenie kto, kiedy i w jakim zakresie miałby dostęp do danych, w tym danych osobowych, oraz jaki jest zakres przyznawanych na tę okoliczność uprawnień, jak również zamieszczenie przez projektodawcę schematu funkcjonujących i projektowanych rozwiązań w zakresie systemu teleinformatycznego. Wymóg ten ma zasadnicze znaczenie z punktu widzenia oceny projektu pod względem zapewnienia ochrony danych osobowych, które znajdą się w systemie spełniającym kryteria systemów określanych jako big data.

Organ do spraw ochrony danych osobowych sceptycznie odniósł się także do rozwiązania polegającego na wprowadzaniu w projekcie ustawy przepisu, zgodnie z którym informacje zawarte w oświadczeniu o stanie majątkowym, są jawne, także co do imienia i nazwiska, z wyjątkiem danych adresowych, informacji o położeniu nieruchomości, a także informacji umożliwiających identyfikację ruchomości komornika. Przepis ten nie określa ograniczenia czasowego publikowanych w tym trybie informacji. Konieczne w tym przypadku jest wyważenie proporcji między interesem publicznym, a ochroną jego prywatności. Istotnym w opisywanym przypadku jest wprowadzenie do przepisów projektowanej ustawy ograniczenia czasowego publikacji w Biuletynie Informacji Publicznej tychże oświadczeń. Okres ten umożliwiłby weryfikację złożonych przez komorników oświadczeń majątkowych, a w przypadku wątpliwości co do ich zgodności z prawem – wszczęcie stosownych postępowań.

Projektodawca częściowo uwzględnił uwagi GIODO. Wskazane zostało, iż zakres informacji zawartych w kwestionariuszu osobowym kandydatów na komorników zostanie uregulowany w rozporządzeniu Ministra Sprawiedliwości. Uregulowano przesłanki, w oparciu o które następuje skreślenie aplikanta komorniczego z listy aplikantów. W ustawie Kodeks postępowania cywilnego dodany został z kolei artykuł, w którym wymienione zostały enumeratywnie kategorie czynności egzekucyjnych podlegających nagrywaniu. W kwietniu 2017 r. projekt skierowany został na Komisję Prawniczą.

CENTRALNE REPOZYTORIUM TRANSAKCJI

Ze względu na projektowany zakres przesyłanych danych (m. in. raportów fiskalnych, paragonów, faktur), w tym danych osobowych (imię i nazwisko lub nazwa podatnika, adres siedziby lub miejsca zamieszkania podatnika, imię i nazwisko posiadacza biletu w przypadku biletów okresowych imiennych), projekt rozporządzenia Ministra Rozwoju w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące[172] był przedmiotem zainteresowania Generalnego Inspektora Ochrony Danych Osobowych. W opiniowanym akcie prawnym projektodawcy zaproponowali stworzenie centralnego repozytorium transakcji, do którego kasy rejestrujące będą raportowały – w postaci elektronicznej – przeprowadzone z ich użyciem transakcje. To oznacza, że **projektowane rozporządzenie swoim zakresem wykracza poza delegację dotyczącą jego wydania**, to ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. Nr 54, poz. 535, z późn. zm.) - w takim zakresie, w jakim projekt dotyczy stworzenia centralnego repozytorium transakcji, do którego kasy rejestrujące będą raportowały przeprowadzane z ich użyciem transakcje. Generalny Inspektor zwrócił również uwagę na przepisy mające na celu tworzenie baz danych zawierających dane osobowe podatników, które to dane będą następnie przetwarzane w centralnych repozytoriach elektronicznych – przy braku określenia czasu ich przetwarzania i celu wykorzystywania zgromadzonych w ten sposób danych. W zależności od zaakceptowanych przez resort wydający przedmiotowe rozporządzenie rozwiązań technicznych co do proponowanych systemów teleinformatycznych przekazujących dane objęte zakresem rozporządzenia i zakres tychże danych, za konieczną do przeanalizowania wydaje się być również forma prawna przyjmowanych rozwiązań – to jest rozważenie czy te zagadnienia (ze względu na stopień ingerencji w prywatność podatnika) nie powinny być jednak uregulowane w ustawie).

Prace nad projektem nie zostały zakończone.

NARODOWE DOBRA KULTURY

Generalny Inspektor opiniował rządowy projekt ustawy o restytucji narodowych dóbr kultury, który w pierwszej wersji, na etapie prac przed skierowaniem projektu do Sejmu, nosił nazwę ustawy o narodowych dobrach kultury[173].

GIODO zgłosił wątpliwości do przepisów projektu ustawy będących delegacjami ustawowymi do wydania rozporządzeń wykonawczych, które określałyby **tryb, sposób i zakres pozyskiwania i wymiany informacji oraz wzajemnych konsultacji pomiędzy przedmiotowymi organami i podmiotam**i z wykorzystaniem danych z systemu IMI w celu odnalezienia

[172] DOLiS-033-400/16.
[173] DOLiS-033-196/16.

i zwrotu dobra kultury oraz w celu jego zabezpieczenia albo mając na względzie potrzebę ochrony dziedzictwa kulturowego oraz zapewnienia bezpieczeństwa obrotu. Generalny Inspektor uznał, że w przepisach rangi ustawy należy doprecyzować jakie konkretnie informacje będą zbierane i przekazywane przez przedmiotowe organy i podmioty, określić czy informacje takie będą zawierać dane osobowe i jaki będzie zakres przetwarzania tych danych.

Kolejne zastrzeżenia organu do spraw ochrony danych osobowych dotyczyły przepisów samej ustawy o restytucji narodowych dóbr kultury jak i przepisów zmieniających ustawę o muzeach i ustawę o bibliotekach. Przedmiotowe przepisy projektodawca skonstruował w ten sposób, że treść przedmiotowych przepisów nie uściślała, jakie konkretnie dane osobowe będą zawierały przedmiotowe wnioski o wydanie pozwoleń i wzory pozwoleń, a część wspólna każdego przepisu wskazywała, że takie wnioski o wydanie pozwoleń i wzory pozwoleń będą zawierać imię i nazwisko autora, posiadacza lub dzierżyciela, a w niektórych przypadkach również adres posiadacza lub dzierżyciela. Generalny Inspektor stwierdził, że tak sformułowane przepisy nie dają pewności co do zakresu wymogu podania określonych danych gdyż pierwsza część każdego przepisu wskazywała na katalog otwarty a druga na zamknięty. GIODO zasugerował enumeratywne określenie – w odpowiednich przepisach projektu ustawy – danych osobowych, które będą zawierały przedmiotowe wnioski o wydanie pozwoleń i wzory pozwoleń.

Ostatnią uwagę Generalny Inspektor wniósł do projektu zmian przepisu ustawy o ochronie zabytków i opiece nad zabytkami, zgodnie z którym w księdze ewidencyjnej, którą ma prowadzić podmiot prowadzący działalność gospodarczą w zakresie obrotu zabytkami na terytorium Rzeczypospolitej Polskiej, umieszcza się odpowiednio: dane zbywcy oraz nabywcy zabytku, a także osób pośredniczących w zbyciu i nabyciu zabytku, w tym osób reprezentujących osoby prawne; dane osoby, na rzecz której została wydana ekspertyza. Również i w tej kwestii GIODO uznał, że należy doprecyzować jakie konkretnie dane osobowe identyfikujące zbywcę, nabywcę, osoby pośredniczące w zbyciu i nabyciu zabytku, osoby reprezentujące osoby prawne, osobę, na rzecz której została wydana ekspertyza będą przetwarzane w przedmiotowej księdze ewidencyjnej.

W wyniku uwag wniesionych przez organ do spraw ochrony danych osobowych projektodawca wyjaśnił wątpliwości odnoszące się do wskazanych w uwagach GIODO przepisów oraz usunął jeden z nich, pozostawiając jednak bez zmian przepis dotyczący delegacji ustawowej do wydania rozporządzenia określającego sposób pozyskiwania wymiany informacji między współpracującymi ze sobą organami i podmiotami w celu odnalezienia i zwrotu dobra kultury oraz w celu jego zabezpieczenia. Generalny Inspektor ponownie wystąpił do projektodawcy o rozważenie uregulowania sposobu i zakresu wymiany informacji między uprawnionymi do współpracy organami.

Ostatecznie wszystkie uwagi Generalnego Inspektora zostały uwzględnione.

RETENCJA DANYCH W REJESTRZE KARTY POLAKA

Generalny Inspektor opiniował również projekt ustawy o zmianie ustawy o Karcie Polaka oraz ustawy o cudzoziemcach (druk nr 904)[174].

[174] DOLiS-033-473/16.

Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę projektodawcy na brak w projektowanych przepisach ograniczenia czasowego przetwarzania danych osobowych osób, których dane osobowe miałyby być przetwarzane w nowo tworzonym rejestrze złożonych wniosków o przyznanie świadczenia pieniężnego dla posiadaczy Karty Polaka oraz decyzji i postanowień wydanych w tych sprawach. GIODO opierał swoje stanowisko na obowiązku zachowania zasady retencji danych przy tworzeniu rejestrów, w których przetwarzane mają być dane osobowe.

Niestety projektodawca nie odniósł się do powyższej uwagi Generalnego Inspektora i nie uwzględnił jej w ostatecznej treści projektu. Ustawa została podpisana przez Prezydenta dnia 29 marca 2017 r. i weszła w życie z dniem 1 stycznia 2017 r., z wyjątkiem art. 1 pkt 6 w zakresie art. 23 ust. 2d oraz art. 2, które wchodzą w życie z dniem 1 stycznia 2018 r.

PARTYCYPACJA SPOŁECZNA W PLANOWANIU PRZESTRZENNYM

Generalny Inspektor opiniował również projekt ustawy – Kodeks urbanistyczno-budowlany[175].

Generalny Inspektor zgłosił swoje uwagi do licznych przepisów, które regulowały publikację dokumentacji lub informacji mogących zawierać dane osobowe, związanych z jawnością i partycypacją społeczną w planowaniu przestrzennym.

Organ do spraw ochrony danych osobowych zwrócił uwagę na zakres danych osobowych widniejących w ogłaszanych dokumentach, który powinien być adekwatny do celu ich publikacji, enumeratywnie określony w projektowanym przepisie oraz okres retencji takich danych. Zatem w celu ochrony danych osobowych osób, których takie dane zawarte będą w dokumentach upubliczniannych czy to w jawnym rejestrze, czy na stronach internetowych Biuletynów Informacji Publicznej bądź np. Wywieszanych na tablicach informacyjnych w urzędach państwowych, należy poddać procesowi anonimizacji pozostawiając w treści jedynie takie dane, które będą adekwatne do celu ich przetwarzania i uniemożliwiające ich identyfikację. W związku z powyższym, Generalny Inspektor zasugerował rozważenie wprowadzenia do projektu kodeksu generalnego zapisu, który określałby proces anonimizacji danych osobowych, zakres takich danych i ich retencję.

GIODO zgłosił również uwagi do przepisów regulujących sposób przeprowadzania dyskusji publicznych i poddał w wątpliwość brak określenia w przepisach rangi ustawowej sposobów utrwalania takich dyskusji (czy będzie miało miejsce zastosowanie wideomonitoringu wraz z nagrywaniem dźwięku, czy będzie to jedynie nagrywanie dźwięku) i ewentualnego późniejszego ich udostępniania.

Generalny Inspektor zgłosił zastrzeżenia także do przepisu, na podstawie którego minister właściwy do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa mógłby powierzyć jednostce nadzorowanej lub podległej wykonywanie zadań związanych z prowadzeniem i utrzymywaniem bazy danych o istniejącym zagospodarowaniu przestrzennym, obejmującą dane pozyskane w wyniku monitorowania przez organy władzy publicznej przy wykorzystaniu systemu teleinformatycznego.

[175] DOLiS-033-466/16.

Organ do spraw ochrony danych osobowych uznał, że przepis ten jest zbyt ogólny aby przyjąć na jego podstawie dopuszczalność powierzenia ustawowego. Projektodawca nie określił jasno zasad, na jakich to powierzenie miałoby mieć miejsce. GIODO wykazał, że aby powierzenie ustawowe było dopuszczalne, właściwe przepisy powinny szczegółowo określać jego warunki oraz granice, w jakich może poruszać się podmiot przetwarzający dane. Jednocześnie nadal będzie on obowiązany do przestrzegania zasad wynikających z przepisów ustawy o ochronie danych osobowych, w tym dotyczących właściwego zabezpieczenia danych.

Ostania część opinii Generalnego Inspektora Ochrony Danych Osobowych do projektu Kodeksu urbanistyczno-budowlanego zawierała stanowisko do przepisów księgi odnoszącej się do stworzenia i działania Rejestru urbanistyczno-budowlanego. Satysfakcjonujący dla GIODO był przepis, która zagwarantował, że dane i informacje gromadzone w Rejestrze będą jawne, z wyłączeniem danych osobowych.

GIODO postulował zmianę i uzupełnienie przepisów księgi tworzącej Rejestr urbanistyczno-budowlany, o przepisy uszczegóławiające sposób prowadzenia Rejestru w systemie teleinformatycznym, który miałby zawierać kwestie dotyczące: podmiotu prowadzącego Rejestr (określenia administratora danych osobowych widniejących w Rejestrze), zakresu informacji gromadzonych w Rejestrze (zakresu przetwarzanych danych osobowych adekwatnie niezbędnych do celu ich przetwarzania), sposób udostępniania, informacji zawartych w Rejestrze innym podmiotom oraz uaktualniania i usuwania danych z Rejestru, w tym okresów przechowywania danych. Powyższe stanowisko Generalny Inspektor argumentował wskazując, że rozporządzenie nie może samodzielnie (w oderwaniu lub w swego rodzaju „uzupełnieniu" przepisów Kodeksu urbanistyczno-budowlanego) kreować określonych zasad przetwarzania danych albo kompetencji organów.

Projektodawca nie odniósł się do powyższych uwag Generalnego Inspektora. Aktualnie prace legislacyjne nad przedmiotową ustawą nie zostały zakończone i procedowane są na etapie konsultacji społecznych i uzgodnień międzyresortowych.

DANE PODATNIKÓW WE WŁADANIU SPÓŁKI MAJĄCEJ REALIZOWAĆ PROJEKTY INFORMATYCZNE

Odnosząc się do dokumentu pt. projekt ustawy o szczególnych zasadach wykonywania niektórych zadań z zakresu informatyzacji administracji podatkowej i kontroli skarbowej[176] Generalny Inspektor oponował przeciw utworzeniu spółki mającej realizować projekty informatyczne oraz wyposażać administrację podatkową w systemy teleinformatyczne lub urządzenia informatyczne lub oprogramowanie do analizy prawdopodobieństwa wystąpienia naruszenia prawa podatkowego i szczątkowej regulacji zasad jej działania. **Generalny Inspektor przypominał, iż przetwarzanie danych podatników przez organy administracji publicznej i ewentualne przekazywanie takich zadań do innych podmiotów powinno być szczegółowo uregulowane w przepisach ustawowych**, gdyż tego wymagają przepisy art. 7 (zasada legalizmu) i art. 51 Konstytucji (prawo do ochrony danych osobowych). Ze względu na ww. niejasności projektu nie było możliwym dokonanie oceny zgodności z zasadą proporcjonalności ujętą w art. 31 ust. 3 Konstytucji. Negatywnie organ

[176] DOLiS-033-39/16.

ds. ochrony danych osobowych ocenił także przekazywanie spółce zadań na podstawie umowy, a nie w ramach przepisów prawa powszechnie obowiązującego. **Krytykowany był także dostęp oraz przetwarzanie danych podatników przez spółkę w celu zapewnienia organom administracji podatkowej narzędzi do analizy prawdopodobieństwa wystąpienia naruszenia prawa podatkowego**. Organ wskazał, że w celu opracowania narzędzi do analizy prawdopodobieństwa wystarczające byłoby uzyskanie dostępu do struktury danych, które byłyby przetwarzane/poddawane analizie przy wykorzystaniu ww. narzędzi, nie zaś do treści ww. danych. W nawiązaniu do powyższego GIODO zauważył, że opracowane przez stowarzyszenie ISACA, dobre praktyki w zakresie projektowania systemów informatycznych zakazują wykorzystywania rzeczywistych danych z systemów informatycznych w środowisku deweloperskim wykorzystywanym do testowania aplikacji. Za daleko idącą i nieuzasadnioną propozycję organ uznał propozycję wyłączenia obowiązku rejestracji przez spółkę tworzonych zbiorów danych oraz zwrócił uwagę, że projekcie nie przewidziano także okresów retencji danych podatników przez spółkę.

Niestety, większość uwag organu ds. ochrony danych osobowych nie znalazła odzwierciedlenia w uchwalonej ustawie. Miało to miejsce także z uwagi na przyjętą przez Sejm RP ścieżkę prac legislacyjnych. W dniu 12 kwietnia 2016 r. odbyło się pierwsze czytanie projektu ustawy, skierowanie projektu pod obrady Komisji Finansów Publicznych oraz przekazanie projektu do zaopiniowania przez właściwe podmioty. Do Biura Generalnego Inspektora projekt wpłynął w dniu 18 kwietnia br. Natomiast już 13 kwietnia odbyło się posiedzenie Komisji Finansów Publicznych i przyjęcie sprawozdania, które stało się podstawą decyzji Sejmu o uchwaleniu projektu w dniu 29 kwietnia. Z uwagi na tak szybkie procedowanie niemożliwym było przedstawienie stanowiska organu ds. ochrony danych osobowych niższej izbie parlamentu we właściwym czasie. W **opinii Generalnego Inspektora nad projektem nie odbyła się wyczerpująca debata publiczna, która powinna mieć miejsce w przypadku propozycji przetwarzania danych osobowych na tak dużą skalę.**

MONITORING NA KOLEI

W zakresie uwag do rządowego projektu ustawy o Straży Ochrony Kolei[177] **organ ds. ochrony danych ocenił propozycje uprawnienia Straży Ochrony Kolei do obserwowania i rejestrowania obrazu oraz dźwięku**. Organ wskazał, że obserwacja powinna być prowadzona przede wszystkim na terenie obszaru kolejowego wyłącznie w niezbędnych przypadkach, kiedy inne metody zbierania informacji albo dowodów nie mogą być zastosowane – przede wszystkim przez samych strażników. **GIODO podkreślił także potrzebę wyczerpującego wskazania metod, jakimi osoby obserwowane będą informowane o stosowaniu monitoringu wizyjnego i podsłuchiwania**. Dotyczy to w szczególności urządzeń znajdujących się na dworcach kolejowych, przystankach oraz w pociągach oraz kamer używanych przez strażników. Regulacja ustawowa powinna określać także metody zapewniania dostępu do nagrań przez osoby obserwowane, okresów przechowywania nagrań i sposobów ich usuwania. Aktualne w tym zakresie pozostają uwagi zgłoszone przez organ ds.

[177] DOLiS-033-141/16.

ochrony danych osobowych do projektu założeń do ustawy o monitoringu wizyjnym[178].

Generalny Inspektor zasugerował także projektodawcy przeprowadzenie analizy niezbędności i oceny wpływu na prywatność prowadzenia przez SOK obserwacji i nagrywania dźwięku, zbierania i przetwarzania danych daktyloskopijnych oraz DNA. Ich wyniki powinny być ujęte w uzasadnieniu i ocenie skutków regulacji, tak by wykazać, iż nie ma innych środków, którymi można by osiągnąć cele postawione przed nową służbą mundurową. Organ wskazał, że pod uwagę powinny w tym kontekście zostać wzięte zasady proporcjonalności oraz celowości ujęte w powszechnie obowiązujących przepisach o ochronie danych osobowych. Konieczna była także odpowiedź na pytanie, czy materiały powyższe będą przekazywane Policji, która zgodnie z przepisami prowadzi właściwe bazy danych. W takim przypadku konieczne było wprowadzenie przepisów o trybie wymiany informacji.

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

ANONIMIZACJA DANYCH NA POTRZEBY STATYSTYKI PUBLICZNEJ

Odnosząc się do dokumentu pt. projekt ustawy o zmianie ustawy o ewidencji ludności, ustawy o opłacie skarbowej oraz ustawy – Prawo o aktach stanu cywilnego[179] **Generalny Inspektor oponował przeciw projektowanym przepisom, w których zaproponowano przekazywanie danych dotyczących stanu zdrowia dzieci, informacji o ciąży i porodzie, poprzednich ciążach i porodach matki, miejscu zamieszkania rodziców dziecka, wykształcenia rodziców, szeroko pojętych danych dotyczących zgonów itp**. Przede wszystkim GIODO zwrócił uwagę, iż projekt powinien być doprecyzowany w zakresie przekazywania tylko zbiorczych informacji zanonimizowanych. Powinny one być wystarczające do celów prowadzenia statystyki publicznej. Opiniowane brzmienie wskazywało na przekazywanie danych osób zidentyfikowanych, co nie jest zgodne z w/w zasadą adekwatności danych.

Po drugie GIODO zauważył, iż w omawianym zakresie uzasadnienie do projektu opisywało historię konsultacji pomiędzy odpowiednimi ministerstwami oraz Głównym Urzędem Statystycznym, pomijając całkowicie kwestie celów, jakim służyć miały te dane po przekazaniu służbom statystyki publicznej. Nie wskazano np. do prowadzenia jakich badań statystycznych określonych w przepisach prawa, takie dane będą potrzebne. GIODO podkreślił, że bez wyczerpującego wskazania celów przetwarzania danych w proponowanych formach, nie było możliwości dokonania oceny niezbędności ich przetwarzania. Organ ds. ochrony danych osobowych sugerował projektodawcy uzupełnienie uzasadnienia do projektu. Wątpliwość budziło także niedookreślenie zakresu informacji np. o osobach stwierdzających zgony. W tym zakresie wskazał na konieczność doprecyzowania przepisów, gdyż bez wyczerpującego wskazania zakresu danych nie ma możliwości dokonania niezbędności ich przetwarzania.

Projektodawca przychylił się do stanowiska organu ds. ochrony danych .

[178] Opinia z dnia 13 sierpnia 2014 r. – sygn. DOLiS-033-523/13/KK/63260/14, http://legislacja.rcl.gov.pl/docs//1/200701/200707/200710/dokument124074.pdf

[179] DOLiS-033-604/16.

6. Interpretacja przepisów

Działalność Generalnego Inspektora Ochrony Danych Osobowych w zakresie interpretacji przepisów prawa dotyczących problematyki ochrony danych osobowych niewątpliwie pozostaje bardzo istotną z punktu widzenia obywateli działalnością. Ta forma działalności edukacyjnej – odpowiedzi na pytania, nie została określona w przepisach kompetencyjnych Generalnego Inspektora. Przepisy nie stanowiąc obowiązku udzielania odpowiedzi nie reglamentują tej formy działalności przepisami chociażby Kodeksu postępowania administracyjnego.

Generalny Inspektor docenia jednak otrzymywane sygnały dotyczące problemów związanych z interpretacją przepisów prawa. Ich treść stanowi częsty impuls do rozważenia podjęcia określonych działań z urzędu (np. Wystąpienia do administracji rządowej, wyjaśnienia i poradniki dostępne na stronie GIODO, tym bardziej, że tematyka wpływających do Biura GIODO zagadnień obejmuje niemal wszystkie dziedziny życia publicznego.

W 2016 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło łącznie 3325 pism zawierających pytania z zakresu ochrony danych osobowych.

Wartym zauważenia jest, iż liczba zapytań dotyczących interpretacji przepisów prawa w 2016 r. W porównaniu do roku 2015 zmniejszyła się o 16%.

W poszczególnych miesiącach analizowanego okresu sprawozdawczego do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła następująca liczba pytań: styczeń: 224, luty 334, marzec 314, kwiecień 314, maj 233, czerwiec 282, lipiec 313, sierpień 253, wrzesień 354, październik 264, listopad 239, grudzień 201.

Zauważyć trzeba, że wciąż duża jest liczba zapytań nadsyłanych przez podmioty profesjonalnie (zawodowo) zajmujące się udzielaniem porad prawnych, jak i administratorów bezpieczeństwa informacji, czyli osoby, które powinny dysponować odpowiednią wiedza 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.

W opisywanym okresie sprawozdawczym, na stronie internetowej urzędu opublikowany został komunikat[180], w którym Generalny Inspektor Ochrony Danych Osobowych przypomniał, iż co do zasady nie zajmuje stanowiska i nie wydaje opinii, w tym wstępnych, dotyczących legalności przetwarzania danych w hipotetycznych sytuacjach przedstawianych w kie-

[180] http://www.giodo.gov.pl/1520223/id_art/8342/j/pl/

rowanych do niego pismach. Stosowanie i interpretacja unormowań ustawy o ochronie danych osobowych należy w pierwszej kolejności do administratorów danych wspieranych przez powołanych administratorów bezpieczeństwa informacji, działy prawne oraz osoby świadczące fachową pomoc prawną. Rolą Generalnego Inspektora jest bowiem kontrola procesu przetwarzania danych osobowych, a nie świadczenie pomocy prawnej. To administrator danych decyduje o celach i środkach przetwarzania, a zatem obowiązany jest respektować wszelkie nałożone na niego przepisami prawa obowiązki związane z procesem przetwarzania danych osobowych. Potwierdza to art. 36b ustawy o ochronie danych osobowych, który stanowi, że w razie niepowołania administratora bezpieczeństwa informacji, administrator danych sam wykonuje zadania określone w art. 36a ust. 2 pkt 1, a więc także zapewnianie przestrzegania przepisów o ochronie danych osobowych.

Podobnie jak w latach poprzednich, także w roku 2016, 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:

- **administracji i sądownictwa** – pytania dotyczące upubliczniania danych osobowych, w tym na stronach internetowych. Pojawiały się ponadto pytania o dopuszczalność przekazywania danych osobowych innym instytucjom publicznym oraz osobom prywatnym. Zgłaszane wątpliwości dotyczyły również ustalenia, jaka jednostka samorządu terytorialnego jest w konkretnym przypadku administratorem danych oraz możliwości zawierania umów powierzenia przetwarzania danych między takimi podmiotami. Pojawiały się zapytania dotyczące udostępniania danych osobowych pomiędzy stronami postępowań cywilnych, a także prawa dostępu do danych zawartych w aktach spraw sądowych.
- **szkolnictwa** – np. pytania dotyczące monitorowania losów absolwentów czy dostępu do dokumentacji przez organ sprawujący nadzór nad szkołą, stosowania monitoringu wizyjnego, czy organizacji procesu przetwarzania danych osobowych, zwłaszcza ze względu na perspektywę rozporządzenia ogólnego o ochronie danych osobowych.
- **służby zdrowia** – w odniesieniu do podstaw przetwarzania danych o stanie zdrowia, w tym pozyskiwania takich danych np. przez pracodawcę, czy też udostępniania i przechowywania dokumentacji medycznej. Pojawiło się ponadto zagadnienie stosowania wideomonitoringu w placówkach ochrony zdrowia oraz możliwości nagrywania przebiegu porad lekarskich.
- **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, np. komornikom. 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 związków zawodowych.

- **mieszkalnictwa –** zapytania zarówno od zarządów, jak i członków wspólnot oraz spółdzielni mieszkaniowych, dotyczące przetwarzania danych osobowych, w tym pozyskiwania danych osób zajmujących lokale, w związku z zarządzaniem nieruchomościami, w tym także lokalami komunalnymi
- **telekomunikacji i Internetu** – pojawiały się np. 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. Kierowane do GIODO zapytania dotyczyły również pozyskiwania danych przez operatorów telekomunikacyjnych w związku z wprowadzeniem obowiązku rejestracji kart prepaid.

Dodatkowo, spośród sygnalizowanych Generalnemu Inspektorowi problemów, szczególną uwagę należy zwrócić na następujące zagadnienia.

PRZEKAZYWANIE DANYCH OSOBOWYCH NIEZASZCZEPIONYCH PACJENTÓW

Wątpliwości co do istnienia podstawy prawnej do udostępnienia danych osobowych niezaszczepionych pacjentów powiatowym inspektorom sanitarnym przez podmioty lecznicze były wiele razy zgłaszane Generalnemu Inspektorowi Ochrony Danych Osobowych. GIODO w przedmiotowej sprawie zajął stanowisko, iż podstawa prawna do tego typu działań znajduje się w przepisach ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, zgodnie z którymi osoby przebywające na terytorium Rzeczypospolitej Polskiej obowiązane są do poddawania się szczepieniom ochronnym. Organy Państwowej Inspekcji Sanitarnej zaś zostały powołane do sprawowania nadzoru nad wykonywaniem obowiązku szczepień i są one uprawnione do dochodzenia wykonania obowiązku szczepień na drodze postępowania egzekucyjnego w administracji. W tym celu zgodnie z prawem, Organy Państwowej Inspekcji Sanitarnej muszą być informowane przez prowadzących szczepienia ochronne o wykonaniu lub niewykonaniu obowiązku szczepień. Osoby przeprowadzające szczepienia ochronne są zobowiązane do prowadzenia dokumentacji medycznej dotyczycącej obowiązkowych szczepień ochronnych, w tym przechowywania karty uodpornienia oraz dokonywania wpisów potwierdzających wykonanie szczepienia i sporządzania sprawozdania z przeprowadzonych obowiązkowych szczepień ochronnych oraz sprawozdania ze stanu zaszczepienia osób objętych profilaktyczną opieką zdrowotną, które przekazują państwowemu powiatowemu inspektorowi sanitarnemu.

W rozporządzeniu Ministra Zdrowia z dnia 18 sierpnia 2011 r. w sprawie obowiązkowych szczepień, wskazuje się zaś, że kwartalne sprawozdanie z przeprowadzonych obowiązkowych szczepień ochronnych jest sporządzane i przekazywane przez osoby przeprowadzające obowiązkowe szczepienia ochronne państwowemu powiatowemu inspektorowi sanitarnemu, w terminie 7 dni po zakończeniu kwartału, za pomocą środków komunikacji elektronicznej albo listem poleconym.

Jednak wobec kształtu przedmiotowych regulacji, które mogą powodować wątpliwości interpretacyjne, a w szczególności wobec faktu,

iż zestawienia danych osób, które nie poddały się szczepieniom tworzone są na podstawie nieprecyzyjnego i niewystarczającego sformułowania „imienny wykaz" o którym mowa w załączniku nr 4 do przedmiotowego rozporządzenia, co nie stwarza pełnych gwarancji ochrony wrażliwych danych osobowych, Generalny Inspektor Ochrony Danych Osobowych skierował wystąpienie[181] do Głównego Inspektora Sanitarnego oraz do Ministerstwa Zdrowia z postulatem o wyraźne uregulowanie w przepisach rangi ustawy kwestii przekazywania przez podmioty lecznicze informacji o niezaszczepionych pacjentach do PPIS. W odpowiedzi na inicjatywę GIODO, Główny Inspektor Sanitarny zapewnił, iż podejmie działania zmierzające do precyzyjnego uregulowania przedmiotowych przepisów.

PRZESYŁANIE NIERZETELNYCH INFORMACJI O „OBOWIĄZKU REJESTRACJI w GIODO"

Do Biura Generalnego Inspektora docierały liczne sygnały od osób, które otrzymywały nierzetelne i nieprawdziwe informacje, które nawoływały do dokonywania „rejestracji firm" w GIODO, wskazując jednocześnie rzekomo losowo wybrane linki do kancelarii/podmiotów które świadczą usługi związane z przetwarzaniem danych osobowych w firmach. W związku z powyższym GIODO skierował do organów ścigania zawiadomienie o podejrzeniu popełniania przestępstwa oszustwa.

WSPOMAGANIE RATUNKOWE PACJENTA

Generalny Inspektor Ochrony Danych Osobowych wypowiedział się w sprawie projektu „Wspomagania Ratunkowego Pacjenta", który sugerował utworzenie bazy danych osób starszych a także chętnych mających problemy zdrowotne, w których znalazłyby się dane m.in. o schorzeniach pacjenta. Wskazał, iż w aktualnym stanie prawnym brak jest przepisów, które legalizowałyby przedmiotowe przedsięwzięcie. Zaznaczył, iż w celu wprowadzenia w życie rozwiązań, polegających na stworzeniu systemu informacyjnego o stanie zdrowia pacjenta, który usprawniłby funkcjonowanie służb ratowniczych, konieczne jest uregulowanie powyższych rozwiązań w przepisach prawa. GIODO zadeklarował również chęć współpracy celem wypracowania właściwych przepisów prawa w tym zakresie, jeżeli podjęte zostaną prace legislacyjne zmierzające do uregulowania przedmiotowego zagadnienia.

POZYSKIWANIE KOPII ALBO SKANÓW DOKUMENTÓW TOŻSAMOŚCI

W analizowanym okresie sprawozdawczym ważnym tematem licznych zapytań napływających do Biura GIODO była kwestia pozyskiwania kopii albo skanów dokumentów tożsamości przez podmioty zarówno publiczne, jak i prywatne z różnych sektorów. Przykładem tu może być sektor bankowy, sektor telekomunikacyjny, portale społecznościowe, kluby czy obiekty sportowe, jak np. stoki narciarskie czy lodowiska. Jednocześnie należy w tym miejscu odesłać do komunikatu Generalnego Inspektora, w kwestii pozyskiwania kopii dokumentów tożsamości klientów przez firmy telekomunikacyjne, zamieszonego na stronie http://giodo.gov.pl/259/id_art/9900/j/pl .

Z otrzymanej korespondencji nasuwają się wnioski, że administratorzy danych pozyskują

[181] http://www.giodo.gov.pl/1520254/id_art/9843/j/pl/

kopie, czy też skany dokumentów tożsamości w celu potwierdzenia tożsamości osoby, albo zastępują konieczność spisania danych łatwiejszą dla nich formą poprzez zrobienie kopii dokumentu, czy szybszą przy ustalaniu danych na odległość metodą pozyskiwania skanu. Częstym przypadkiem pozyskiwania od klienta kopii dokumentu tożsamości, jest sytuacja, gdy dochodzi do zawarcia umowy za pośrednictwem zdalnych kanałów sprzedaży, i niejednokrotnie przekazanie kopii dokumentu tożsamości warunkuje możliwość zawarcia tego typu umowy. Są też sytuacje, że przekazanie kopii dokumentu tożsamości pozwala klientowi na skorzystanie z oferty promocyjnej. Takie działanie należy uznać za prowadzące do obejścia przepisów prawa, a tym samym nieakceptowalne.

Stanowisko Generalnego Inspektora od dłuższego czasu bowiem pozostaje niezmienne w tej kwestii, i o ile sam sposób pozyskiwania danych osobowych jest z punktu widzenia ustawy o ochronie danych osobowych obojętny (por. Wyrok Naczelnego Sądu Administracyjnego z dnia 19 grudnia 2001 r.; sygn. akt II SA 2869/00, czy też wyrok NSA z dnia 7 listopada 2003 r.; sygn. akt II SA 1432/02), to pozyskanie danych w takim zakresie jaki znajduje się na skopiowanym/zeskanowanym dokumencie tożsamości powinno mieć podstawę prawną w przepisach prawa, pozyskane dane powinny być adekwatne do realizacji zamierzonego celu, a także usuwane niezwłocznie po wykorzystaniu. Zdarza się bowiem, że nawet jeżeli podmiot legitymuje się podstawą prawną do pozyskania wszystkich danych zawartych w dokumencie tożsamości i wszystkie pozyskane dane są adekwatne i niezbędne do realizacji zamierzonego celu przetwarzania danych, to administrator danych zapomina o usunięciu tych danych po ich wykorzystaniu, naruszając tym samym przepisy dotyczące ograniczenia czasowego przechowywania danych. Reasumując przetwarzanie danych z dowodu osobistego będzie zatem zgodne z prawem, jeśli przetwarzanie wszystkich danych pochodzących z tego dokumentu będzie znajdowało stosowną podstawę prawną, nie będzie prowadziło do gromadzenia danych w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są przetwarzane. Jednocześnie, co istotne, przetwarzanie danych nie może odbywać się w sposób, który narusza obowiązujące przepisy prawa.

REALIZACJA PROGRAMU 500+

Wiele kierowanych do Generalnego Inspektora **zapytań dotyczyło stosowania w praktyce przepisów ustawy o pomocy państwa w wychowaniu dzieci (realizacji programu 500+). Celem wyjaśnienia zgłaszanych** mu wątpliwości, GIODO opublikował na stronie internetowej urzędu komunikaty dotyczące:

- składania wniosków o świadczenie 500+ przez Internet http://www.giodo.gov.pl/560/id_art/9254/j/pl/
- zgłaszania zbiorów do rejestracji GIODO w związku z realizacją Programu Rodzina 500+ http://www.giodo.gov.pl/560/id_art/9154/j/pl/
- nowelizacji ustawy o ochronie danych osobowych http://giodo.gov.pl/560/id_art/9121/j/pl/

Problemy interpretacyjne dotyczyły zwłaszcza określenia administratora danych, w tym w kontekście nowego art. 23 ust. 2a ustawy o ochronie danych osobowych, wprowadzającego pojęcie „jednego administratora". Zgłaszane były również wątpliwości związane z możliwością udostępniania całych zbiorów

danych, w przypadku gdy np. udzielaniem świadczeń rodzinnych zajmuje się ośrodek pomocy społecznej, a wychowawczych urząd gminy.

Generalny Inspektor wyjaśniał wówczas, iż w takiej sytuacji występuje dwóch niezależnych administratorów danych, przetwarzających dane na potrzeby realizacji dwóch różnych celów. Udostępnienie danych osobowych między nimi musiałoby znajdować oparcie w jednej z przesłanek określonych w art. 23 ust. 1 ustawy o ochronie danych osobowych – jeśli chodzi o dane osobowe tzw. Zwykłe (jak np. imię, nazwisko, adres zamieszkania), bądź też w art. 27 ust. 2 – w odniesieniu do danych szczególnie chronionych, których zamknięty katalog określony został w art. 27 ust. 1 ustawy. Tymczasem żaden przepis ustawy o pomocy państwa w wychowywaniu dzieci nie zezwala na działania polegające na przekazywaniu w całości bazy danych zgromadzonych w innym celu przez inny podmiot – brak jest zatem podstaw prawnych dla tego rodzaju działań. GIODO zauważył, iż samo nadanie upoważnienia do prowadzenia postępowań w sprawie świadczenia wychowawczego i wydawania w tych sprawach decyzji (o którym mowa w art. 10 ust. 2 ustawy o pomocy państwa w wychowywaniu dzieci) nie oznacza uprawnienia do pozyskiwania od innych podmiotów całych zbiorów danych osobowych prowadzonych dla potrzeb realizacji innych zadań.

Nie wyklucza to oczywiście prawa do pozyskiwania danych w indywidualnych sprawach, na potrzeby konkretnego postępowania, którego nie należy utożsamiać z udostępnianiem danych osobowych „na zapas". Zasięganie informacji od innych organów może zatem odbywać się w ramach postępowań wyjaśniających w indywidualnych przypadkach, na postawie przepisów o charakterze ogólnym – ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23, z późn. Zm.) oraz ustawy o pomocy państwa w wychowywaniu dzieci, z wykorzystaniem mechanizmów określonych w przepisach ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114, z późn. Zm.).

WYSYŁANIE NIEZAMÓWIONEJ INFORMACJI HANDLOWEJ (SPAM)

Duża część korespondencji, która wpływa do Biura Generalnego Inspektora Danych Osobowych dotyczy spamu. Osoby otrzymujące niezamówioną informację handlową drogą elektroniczną, której nie zamawiały i na jej otrzymywanie nie wyraziły zgody albo przesyłają w treści swoich pism prośby o pomoc w takich sprawach i interwencję GIODO albo przesyłają do wiadomości Generalnego Inspektora pełną wymianę korespondencji z takimi firmami.

Niestety zastosowanie ustawy o ochronie danych osobowych w przypadku spamu jest bardzo ograniczone. Pewne środki ochrony przewidują przepisy ustawy o ochronie danych osobowych, dające możliwość wniesienia sprzeciwu wobec przetwarzania danych osobowych w celach marketingowych. Nie mniej jednak GIODO przestrzega, w sformułowanym na stronie internetowej pod adresem: http://www.giodo.gov.pl/361/id_art/8304/j/pl/ komunikacie, że wysłanie zwrotnej informacji ze sprzeciwem na adres, z którego otrzymany został spam, pomoże zidentyfikować konto jako aktywne, co spowoduje, że poczta elektroniczna z jeszcze większym natężeniem będzie atakowana przez programy spamerskie.

Generalny Inspektor sugeruje również w komunikacie aby nie reagować na spam odpowiedzią, odwiedzać podanych w nim adresów, ani podawać dodatkowych danych i zaleca ignorowanie takich maili, dzięki czemu istnieje szansa, że konto nie zostanie rozpoznane przez spamera jako aktywne.

Zważywszy na ogromną ilość pism, jaką GIODO otrzymuje w przedmiotowej sprawie, wydaje się, że obecnie dostępne w powszechnie obowiązujących przepisach prawa środki karne i cywilne dedykowane do walki z problemem spamu są niewystarczające.

MONITORING WIZYJNY

Dość charakterystyczną część korespondencji kierowanej do Generalnego Inspektora Ochrony Danych Osobowych stanowią pytania dot. monitoringu wizyjnego. Obejmują one m.in. nadzorowanie pracowników, uczniów i nauczycieli w szkołach, obserwację przestrzeni wspólnych w blokach mieszkalnych i przestrzeni wokół domów jednorodzinnych. Niejednokrotnie wiąże się to z naruszaniem prywatności poprzez obserwację sąsiadów, osób korzystających z toalet czy zakresem dopuszczalnego nadzoru. Przykładowo pojawia się wiele pytań o możliwość stosowania rejestracji nie tylko obrazu, ale także dźwięku. W tym zakresie mniejszość stanowią zapytania o stosowanie monitoringu przez służby porządku publicznego (fotoradary, systemy monitoringu miejskiego). To raczej swobodne korzystanie z kamer przez przedsiębiorców, szkoły, pracodawców i osoby prywatne rodzi duże wątpliwości obywateli. Przede wszystkim są to problemy związane z objęciem obserwacją kamer terenu należącego do innych osób, dostępu do nagrań czy braku wpływu na podjęcie przez wspólnotę albo członków wspólnoty decyzji o instalacji kamer oraz braku realizacji obowiązku informacyjnego. Poza udzielaniem odpowiedzi na najbardziej palące przypadki, organ ds. ochrony danych osobowych przygotował Wytyczne GIODO dotyczące wykorzystania monitoringu wizyjnego w szkole[182] oraz webinarium Monitoring wizyjny w szkole[183]. Działania te nie są wystarczającą odpowiedzią organów administracji publicznej na problemy związane z ochroną prywatności i danych osobowych osób obserwowanych. Dlatego też konieczne jest jak najszybsze podjęcie prac nad ustawą o monitoringu wizyjnym, która w sposób kompleksowy regulowałaby obowiązki administratorów systemów monitoringu oraz prawa osób obserwowanych. W obliczu rychłego wejścia w życie ogólnego rozporządzenia o ochronie danych osobowych oraz wyroku Trybunału Sprawiedliwości UE w sprawie C-212/13 **Ryneš**[184], funkcjonowanie monitoringu wizyjnego na w oparciu o przepisy ustawy o ochronie danych osobowych nie będzie możliwe.

[182] http://www.giodo.gov.pl/1520056/id_art/9840/j/pl
[183] http://giodo.gov.pl/1520272/id_art/9851/j/pl/
[184] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A62013CJ0212

7. Rejestry prowadzone przez Generalnego Inspektora Ochrony Danych Osobowych

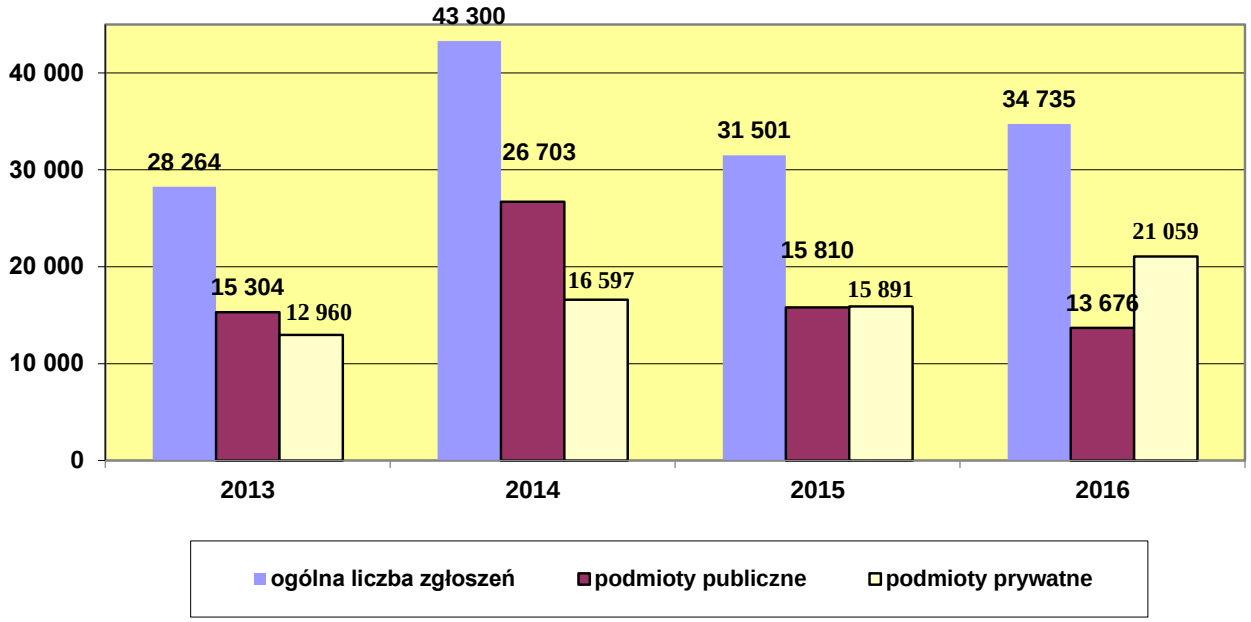
7.1. Rejestracja zbiorów danych osobowych

Praca GIODO w zakresie rejestracji zbiorów danych osobowych lat zdeterminowana rosnącą w bardzo szybkim tempie liczbą wpływających zgłoszeń. Wydawało się, że na mocy zmian 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., dojdzie do zmniejszenia skali tego zjawiska. Wszak z obowiązku rejestracji zbioru danych wyłączeni zostali administratorzy danych przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane szczególnie chronione. Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane szczególnie chronione, nie podlega również administrator danych, który powołał administratora bezpieczeństwa informacji i zgłosił go do rejestracji Generalnemu Inspektorowi. Zakładano, że nowe wyłączenia obowiązku notyfikacji zbiorów danych wpłyną na zmniejszenie ilości zgłoszeń zbiorów danych nadsyłanych do Generalnego Inspektora. Zmiana ustawy nie przyniosła spodziewanych skutków. Mimo wejścia w życie nowelizacji, w 2015 roku wpłynęło więcej zgłoszeń zbiorów danych do rejestracji niż w roku 2013, tendencja wzrostu utrzymała się również w roku 2016. Co więcej, administratorzy danych często nie uwzględniają nowych włączeń z obowiązku rejestracji zbiorów danych i zgłaszają do rejestracji zbiory danych osobowych nie podlegające zgłoszeniu.

Co więcej liczne zmiany w prawie generują lawinowy napływ nowych zgłoszeń zbiorów do rejestracji (np. program rodzina 500+ to około 2 tyś. postępowań), aktualizacji i wniosków o wydanie decyzji o wykreśleniu zbioru z rejestru, np. Zmiany w przepisach meldunkowych.

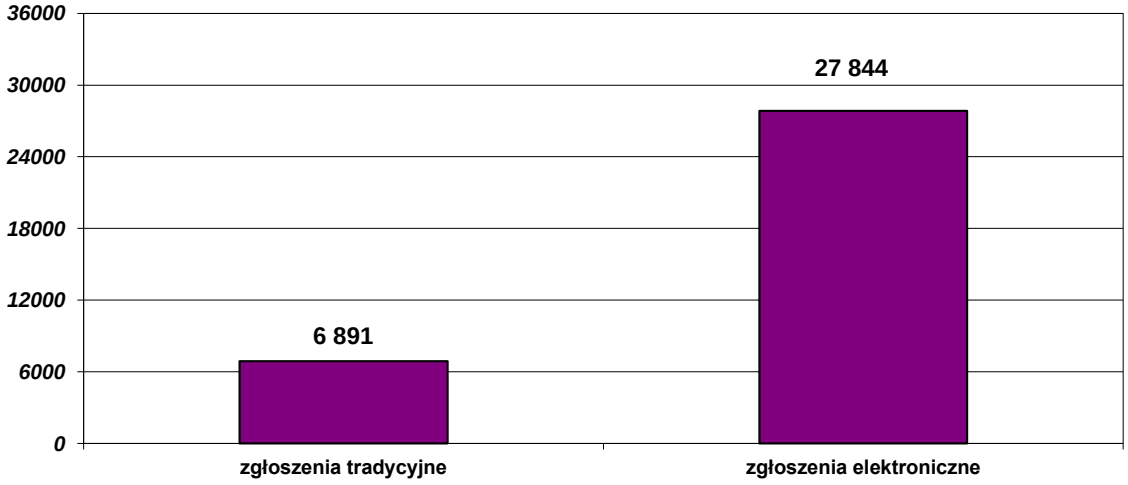
W 2016 roku, administratorzy danych, wypełniając obowiązek określony w art. 40 ustawy o ochronie danych osobowych , zgłosili do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych 34 735 zbiorów danych osobowych.

Podmioty z sektora administracji publicznej zgłosiły 13 676 zbiorów, co stanowi 39% ogólnej liczby zgłoszeń dokonanych w tym okresie (spadek o 10% w stosunku do 2015 r.), a podmioty z sektora prywatnego 21 059 zbiorów, co stanowi 61% ogólniej liczby zgłoszonych zbiorów (wzrost o 10% w stosunku do 2015 r.). Ta wzrostowa tendencja kształtowała się od rekordowego roku 2014 i obecnie w znacznym stopniu ilość zbiorów danych zgłoszonych przez przedsiębiorców przewyższa liczbę zbiorów od podmiotów publicznych.



Wykres 15. ***Liczbowe zestawienie zbiorów danych zgłoszonych do rejestracji w latach 2013 -2016.***

W 2016 roku **27 844** zgłoszenia dokonano drogą elektroniczną przy użyciu programu wspomagającego, udostępnionego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych. Zgłoszenia dokonane drogą elektroniczną stanowiły 80% wszystkich zgłoszeń, które wpłynęły do Biura Generalnego Inspektora Ochrony Danych Osobowych w 2016 roku. Widoczna jest zatem równomierna tendencja wzrostowa w stosunku do lat ubiegłych (2015 r. – 77%, 2014 r. – 75%, 2013 r. – 73%).



Wykres 16. ***Liczbowe zestawienie zgłoszeń zbiorów danych do rejestracji dokonywanych w 2015 r. W formie tradycyjnej i elektronicznej.***

Liczba zakończonych postępowań prowadzonych w związku ze zgłoszeniami zbiorów do rejestracji w okresie sprawozdawczym wyniosła **9 456.** 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 8 142 zbiorów.**

Stosunkowo często informacje zawarte w zgłoszeniu nie pozwalały na zakończenie sprawy bez przeprowadzenia postępowania wyjaśniającego. W 2016 roku w toku postępowań rejestracyjnych do wnioskodawców **skierowano 968 pism**, 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[185].

W 2016 roku wysłano do wnioskodawców **729 pism informujących o braku obowiązku zgłoszenia do rejestracji zbioru**, wynikającym z przesłanek określonych w art. 43 ust. 1 i 1a ustawy oraz **585 informacji o braku podstaw do dokonania wpisów w rejestrze z innych przyczyn** (dotyczyły one zgłoszeń dokonanych przez podmioty nie będące administratorami danych lub zgłoszeń obejmują-

[185] W roku 2016 z obowiązku zgłoszenia zbioru danych osobowych do rejestracji zwolnieni byli administratorzy danych:
1) zawierających informacje niejawne,
1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,
2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym,
2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej,
2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej,
2c) przetwarzanych przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej,
3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,
4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,
5) dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,
6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,
7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
9) powszechnie dostępnych,
10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego,
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.

cych więcej niż jeden zbiór danych osobowych, a także zgłoszeń dotyczących danych, w stosunku do których przepisy ustawy nie mają zastosowania).

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 z późn. zm.). W konsekwencji w 2016 roku skierowano do wnioskodawców, na podstawie art. 64 § 2 Kodeksu postępowania administracyjnego**,** 309 wezwań do uzupełnienia w zgłoszeniu braków formalnych.

Jeżeli zgłoszenie pozytywnie przejdzie wstępną weryfikację, 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 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. Z**astosowanie 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.

W okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych wydał **14 decyzji o odmowie rejestracji zbioru danych. Żaden z administratorów danych nie złożył wniosku o ponowne rozpatrzenie sprawy.** Najczęściej decyzje te nakazywały usunięcie danych nieadekwatnych do celu przetwarzania. 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 2016 r., poz. 599 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.

Zdarza się, że w toku postępowania prowadzonego w związku ze zgłoszeniem zbioru danych do rejestracji wnioskodawca cofa zgłoszenie np. informując, że zrezygnował z utworzenia zbioru danych osobowych. W takich sytuacjach postępowanie rejestracyjne staje się bezprzedmiotowe i konieczne jest wydanie decyzji o jego umorzeniu. W **2016 roku wydanych zostało 117 decyzji o umorzeniu postępowania rejestracyjnego.**

Zadania GIODO związane z prowadzeniem rejestru zbiorów danych osobowych obejmują również rozpatrywanie zgłoszeń aktualizacyjnych, tj. Zgłoszeń zmian informacji zawartych w zgłoszeniu rejestracyjnym[186] 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 2016 roku **rozpatrzone zostały 464 zgłoszenia aktualizacyjne** dokonane przez administratorów danych na podstawie art. 41 ust. 2 ustawy. Ponadto Generalny Inspektor Ochrony Danych Osobowych wydał **34 decyzje o wykreśleniu zbioru** danych z ogólnokrajowego, jawnego rejestru zbiorów danych osobowych z powodu zaprzestania przetwarzania danych w zbiorze. Należy przy tym zaznaczyć, iż decyzja, o której mowa powyżej może dotyczyć więcej niż jednego zbioru danych osobowych.

W ramach wykonywania zadania ustawowego polegającego na informowaniu o zarejestrowanych zbiorach Generalny Inspektor Ochrony Danych Osobowych **wydał w omawianym okresie 5 534 zaświadczenia o zarejestrowaniu zbioru danych**. Dla porównania w 2015 roku zostało wydanych 1 977 zaświadczeń, co oznacza wzrost w liczbach bezwzględnych o 3 557 zaświadczeń, tj. Wzrost o 178%. Znaczący wzrost liczby wydanych zaświadczeń wynikał z rozpatrywania w pierwszej kolejności zbiorów, w których są przetwarzane dane szczególnie chronione. W przypadku zarejestrowania zbioru danych, w którym przetwarzane są dane osobowe szczególnie chronione, określone w art. 27 ust. 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych wydaje zaświadczenie z urzędu, niezwłocznie po dokonaniu rejestracji takiego zbioru[187]. Ponadto Administrator danych może także wystąpić z wnioskiem do Generalnego Inspektora Ochrony Danych Osobowych o wydanie zaświadczenia o zarejestrowaniu zbioru[188].

Rok 2016 był jednym z ostatnich lat, w których obowiązuje model rejestracji zbiorów danych osobowych, z jakim mamy do czynienia na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Odejdzie on do historii z dniem 25 maja 2018 r.

Od tego dnia, w polskim systemie prawnym, będzie stosowane bezpośrednio ogólne rozporządzenie o ochronie danych. Rozporządzenie zniesie ogólny obowiązek zgłaszania do rejestracji wszystkich operacji przetwarzania danych i kontroli wstępnej w obecnym kształcie, kładąc szczególny na samokontrolę administratora danych już na etapie projektowania operacji przetwarzania. Kontrola organu nadzorczego (po dokonaniu oceny skutków przetwarzania przez administratora) będzie miała miejsce w przypadkach szczególnego

[186] 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.
[187] Art. 42 ust. 4 ustawy.
[188] Art. 42 ust. 3 ustawy.

zagrożenia prywatności osób, których dane dotyczą.

Na realizację zadania GIODO jakim było rozpatrywanie zgłoszeń zbiorów danych osobowych wpływ miała nowelizacja ustawy o ochronie danych osobowych, która weszła w życie 1 stycznia 2015 roku. Ustawa podwyższyła status administratorów bezpieczeństwa informacji, ale oczekiwano także, że w związku z nowymi zadaniami ABI oraz dodatkowymi zwolnieniami z obowiązku rejestracji zbiorów, liczba zgłoszeń do rejestracji spadnie w istotny sposób. Nowelizacja wyszła bowiem naprzeciw postulatom administratorów danych i tendencjom panującym w UE, które znalazły wyraz w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE i zawęziła katalog zbiorów danych jakie administratorzy są obowiązani zgłosić do rejestracji Generalnemu Inspektorowi. Mimo upływu dwóch latach od wejścia w życie zmian, praktyka wskazuje na to, że nie wszyscy administratorzy danych znają te ułatwienia i korzystają z nich. Obecnie, poza zwolnieniami obowiązującymi już przed 1 stycznia 2015 roku, z obowiązku rejestracji zbioru zwolnieni są administratorzy danych przetwarzanych w zbiorach, które nie są prowadzone z wykorzystaniem systemów informatycznych, z wyjątkiem zbiorów zawierających dane szczególnie chronione. Ponadto, jeśli administrator danych nie przetwarza w zbiorze danych szczególnie chronionych, powołał administratora bezpieczeństwa informacji i zgłosił go do rejestracji Generalnemu Inspektorowi, wówczas nie musi zgłaszać takiego zbioru do rejestracji.

Należy jednak podkreślić ogólny wzrost świadomości administratorów danych, zwłaszcza przedsiębiorców, co do zasad przetwarzania danych i obowiązków podmiotów przetwarzających dane osobowe. W 2016 roku administratorzy danych osobowych zgłosili do rejestracji Generalnemu Inspektorowi więcej zbiorów danych niż w roku 2013, czy 2015.

Poza kontrolą wstępną (zwłaszcza w przypadku zbiorów zawierających dane szczególnie chronione) postępowania prowadzone w związku z rozpatrywaniem zgłoszeń zbiorów danych do rejestracji posiadają istotny walor edukacyjny w stosunku do administratorów danych i podmiotów przetwarzających dane osobowe. Obowiązek zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi 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 2016 r. Wysłano do administratorów danych blisko tysiąc informacji w tych sprawach.

7.1.1. Postępowania rejestracyjne dotyczące przetwarzania danych osobowych przez podmioty z sektora prywatnego

W roku 2016 można było zaobserwować rosnącą liczbę zgłoszeń zbiorów prowadzonych w związku z udostępnianiem aplikacji mobilnych, stosowaniem rozwiązań opartych na biometrii oraz przetwarzaniem danych geolokalizacyjnych.

Postępowanie rejestracyjne opiera się na oświadczeniach administratora danych zawartych w treści zgłoszenia, jednak rozpatrzenie tych spraw, ze względu na poziom ich trudności oraz często precedensowy charakter, wymaga zazwyczaj przeprowadzenia postępowania wyjaśniającego. Wnioskodawcy przedstawiają zasady funkcjonowania oferowanych przez siebie usług oraz opisują zastosowane rozwiązania techniczne. Należyta ocena przedstawionych informacji wymaga odpowiedniej wiedzy z zakresu tzw. nowych technologii. Rozumienie technicznych aspektów usług świadczonych przez administratorów danych jest bowiem niezbędne do dokonania oceny m. in. adekwatności zakresu danych do celu ich przetwarzania lub stwierdzenia, czy konkretna informacja stanowi daną osobową, często także ustalenia administratora danych.

PRZETWARZANIE DANYCH OSOBOWYCH w APLIKACJACH MOBILNYCH

Użytkownicy aplikacji mobilnych z reguły nie zdają sobie sprawy, że aplikacje te są w stanie zbierać ogromne ilości danych osobowych z urządzeń wykorzystanych do ich obsługi tj. smartfonów, tabletów, netbooków lub laptopów. Chodzi tu zarówno o dane służące bezpośrednio do zawarcia umowy o korzystanie z aplikacji oraz realizacji tej usługi oraz o dane przechowywane na urządzeniu przez użytkownika, ale także dane geolokalizacyjne, dane dotyczące parametrów życiowych.

Grupa Robocza Artykułu 29 ds. Ochrony Danych w Opinii 2/2013 przyjętej w dniu 27 lutego 2013 r. W sprawie aplikacji mobilnych (WP 202) wyróżniła cztery główne podmioty, które mogą być zaangażowane w rozwój, dystrybucję oraz działanie aplikacji mobilnych – są to twórcy aplikacji (w tym właściciele aplikacji), producenci urządzeń oraz systemów operacyjnych, dystrybutorzy aplikacji, a czwartą grupę stanowią inne strony zaangażowane w przetwarzanie danych osobowych. Zgodnie z treścią powyższej Opinii w niektórych przypadkach obowiązki związane z ochrona danych osobowych są dzielone, w szczególności wtedy jeśli te same podmioty są zaangażowane w wielu etapach.

W związku z powyższym administratorem danych użytkowników aplikacji mobilnych może być zarówno twórca aplikacji, jeżeli przetwarza dane użytkowników dla własnych celów, producenci urządzeń oraz systemów operacyjnych (dane przetwarzane w celu zapewnienia płynności działania urządzenia, korzystania z aplikacji, bezpieczeństwa itd.), czy też sklep z aplikacjami (dane na temat zakupu) lub też w niektórych sytuacjach również podmiot trzeci.

Do rejestracji Generalnemu Inspektorowi zgłoszonych zostało kilkaset (około 300, które w nazwie zawierały „aplikacja", w tym 28 zawierających „aplikacje mobilne") zbiorów danych zawierających dane osób korzystających z takich aplikacji. Zakres danych przetwarzanych w tych zbiorach obejmuje zazwyczaj wyłącznie tzw. dane zwykłe. Najczęściej są to dane w postaci imienia i nazwiska, adresu zamieszkania, adresu poczty elektronicznej, numeru telefonu, adresu IP, pozycji GPS, ID użytkownika, ID urządzenia, daty ważności karty, rodzaju systemu operacyjnego zainstalowanego na urządzeniu, rodzaju pobranej aplikacji.

Jedynie niewielka ilość zgłoszeń dotyczy zbiorów danych, w których przetwarzane są dane szczególnie chronione, o których mowa w art. 27 ustawy o ochronie danych osobowych. W zbiorach tych przetwarzane są dane użytkowników korzystających zazwyczaj ze szczególnego rodzaju aplikacji mobilnych nazywanych „technologiami ubieralnymi", które monitorują stan zdrowia osób korzystających z tych aplikacji. Aplikacje te umożliwiają w szczególności pomiar i monitorowanie parametrów życiowych, przykładowo pulsu, temperatury, poziomu glukozy we krwi. Zatem w zbiorach tych przetwarzane są dane ujawniające bezpośrednio lub w kontekście stan zdrowia, osób których dane te dotyczą.

Jako podstawę prawną upoważniającą do prowadzenia zbiorów danych zawierających dane użytkowników aplikacji mobilnych wnioskodawcy wskazują zazwyczaj zgodę osób, których dane dotyczą (art. 23 ust. 1 pkt 1 ustawy o ochronie danych osobowych). W niektórych zgłoszeniach administratorzy wskazują dodatkowo przesłanki wymienione w art. 23 ust. 1 pkt 3 ustawy,tj. przetwarzanie jest 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 oraz w art. 23 ust. 1 ust. 5 ustawy, tj. przetwarzanie jest niezbędne do wypełnienia prawnie usprawiedliwionych celów.

Główne zagadnienia jakie mogą pojawić się przy rozpatrywaniu zgłoszeń zbiorów danych dotyczących użytkowników aplikacji mobilnych to przede wszystkim ustalenie, jaką funkcję w procesie dystrybucji i wykorzystania aplikacji pełni podmiot zgłaszający zbiór, kwestia podstawy prawnej do przetwarzania danych oraz adekwatność zakresu danych w stosunku do celu ich przetwarzania.

PRZETWARZANIE DANYCH OSOBOWYCH ZWIĄZANE Z ZASTOSOWANIEM ROZWIĄZAŃ OPARTYCH NA BIOMETRII

Do GIODO wpływają zgłoszenia zbiorów danych, w których przetwarzane są dane biometryczne, przy czym w znacznej części administratorami danych przetwarzanych w tych zbiorach są podmioty prywatne. Jak wynika z treści zgłoszeń, do zbiorów danych są pozyskiwane wzorce biometryczne w postaci odcisków palców (obrazów linii papilarnych), obrazów tęczówki oka, geometrii twarzy oraz wzorców podpisu odręcznego.

W części zgłoszeń wskazano, iż zastosowano biometrię multimodalną, stanowiącą połączenie różnych technologii biometrycznych, mając przy tym na celu zwiększenie dokładności czy też skuteczności funkcjonowania systemu. Poprzez multimodalną metodę biometryczną należy zatem rozumieć wykorzystanie co najmniej dwóch modalności biometrycznych (np. obraz linii papilarnych palców rąk oraz obraz siatkówki oka). Systemy biometryczne są ściśle powiązane z określoną osobą, bowiem umożliwiają identyfikację lub uwierzytelnianie przy wykorzystaniu niepowtarzalnych cech.

Należy przy tym dostrzec wzrost liczby zgłoszeń zbiorów danych, w których wykorzystywany jest wzorzec biometryczny. Jest to związane z upowszechnianiem tej metody, która ma zastosowanie zarówno w identyfikacji i uwierzytelnianiu/weryfikacji tożsamości, kontroli wstępu do obszaru o ograniczonym dostępie, autoryzacji osób uprawnionych do podejmowania czynności w imieniu innej osoby (np. do głosowania), czy też identyfikowania osób sprawiających zagrożenie dla bezpieczeństwa i porządku publicznego.

PRZETWARZANIE i DOSTĘP DO DANYCH GEOLOKALIZACYJNYCH

Trzy najważniejsze rodzaje infrastruktury stosowane w celu zapewnienia usług geolokalizacyjnych to: **GPS, WiFi i stacje bazowe GSM.**

Od 2012 roku do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło ok. 20 zgłoszeń zbiorów, w których przetwarzane są dane osobowe w oparciu o dane geolokalizacyjne, w tym ok. 6 zgłoszeń pochodziło od administratorów danych osobowych oferujących usługi z zakresu monitorowania pojazdów GPS, oprogramowanie pozwalające na wygodne zarządzanie flotą pojazdów (kontrola czasu pracy pojazdów i pracowników, kontrola paliwa, zarządzanie ruchem pojazdów w terenie, alerty wysyłane na mail lub sms pozwalają na natychmiastową reakcję na różne zdarzenia dotyczące pojazdów w terenie).

Oferty takie są kierowane zarówno do klientów prowadzących działalność gospodarczą (umożliwia tworzenie Ewidencji Przebiegu Pojazdów zgodnej z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2016 r. poz. 710), wymaganej przez Urzędy Skarbowe, w przypadku zadeklarowania samochodu osobowego do wykorzystywania go wyłącznie do celów prowadzonej działalności gospodarczej, a także dla klientów indywidualnych mających wpływ na poprawę bezpieczeństwa (umożliwiają precyzyjną lokalizację pozycji pojazdu w przypadku kradzieży, sprawdzenie stanu pojazdu oraz miejsca ostatniej zarejestrowanej lokalizacji, unieruchomienie za pomocą komunikatów SMS, powiadomienia o zdarzeniach, alarmach).

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1 i 3 ustawy. Zakres przetwarzanych danych o osobach ogranicza się wyłącznie do danych zwykłych.

W 2014 roku zgłoszony został zbiór przez administratora obsługującego serwis społecznościowy oferujący narzędzia i usługi on-line umożliwiające tworzenie i pobieranie tras GPS z wykorzystaniem aplikacji mobilnych oraz używania technologii mobilnych i rozwiązań internetowych do komunikowania się z innymi uczestnikami społeczności (trasy turystyczne, rowerowe i inne). Jako podstawę prawną przetwarzania danych osobowych administrator wskazał zgodę. W zbiorze przetwarzane są wyłącznie dane zwykłe.

W 2016 roku wpływały także zgłoszenia od administratora danych oferującego usługę aplikacji mobilnej służącej do zamawiania taksówek. Po uruchomieniu aplikacji w telefonie GPS lokalizuje na mapie telefon użytkownika i pokazuje wszystkie taksówki dostępne w okolicy.

Również w 2016 roku wpłynęło ok. 10 zgłoszeń od administratorów danych oferujących obsługę aplikacji mobilnych działających na podobnej zasadzie jak podany wyżej przykład:

- Aplikacja informująca o wydarzeniach i aktywnościach (kulturalne, sportowe, towarzyskie, hobby i inne) w najbliżej okolicy, która wykrywa lokalizację i wyświetla na mapie.
- Aplikacja mobilna na smartfonie z urządzeniem lub urządzeniami beacon, która pozwala na całodobowe kontrolowanie miejsc bądź rzeczy, poprzez system nadajników tworzących strefę, obsługiwaną za pomocą smartfona. Informuje o lokalizacji (np. W przypadku kradzieży).
- Aplikacja pozwalająca dzięki specjalnej opasce kontrolowanie zdrowia innej osoby, również jej lokalizacji w razie wypadku. W przypadku tego zgłoszenia zakres danych wykracza poza dane zwykłe, w odróżnieniu od innych wskazanych przypadków zgłoszeń. Specyfika i cel aplikacji warunkuje przetwarzanie danych związanych ze zdrowiem osoby. Jako podstawę prawną przetwarzania danych osobowych administrator wskazał art. 23 ust. 1 pkt 1 i 3 ustawy, a jako podstawę prawną przetwarzania danych osobowych szczególnie chronionych (stan zdrowia) administrator wskazał art. 27 ust. 2 pkt 1 ustawy, tj. Zgodę na piśmie.
- Aplikacja pozwalająca na ustalenie lokalizacji osoby potrzebującej pomocy w górach.
- Aplikacja pozwalająca ustalić miejsca przyjazne zwierzętom.
- Aplikacja która pomoże załatwić formalności po śmierci bliskiej osoby.
- Aplikacja pozwalająca zamierzyć zgubiony, skradziony telefon.
- Aplikacja pozwalająca odnaleźć restauracje, kawiarnie w okolicy, uzyskać informacje o zniżkach, nabyć zniżki, kupony, rabaty.
- Aplikacja pozwalająca ustalić dojazd do dowolnego miejsca komunikacją miejską.
- Aplikacja skierowana do rowerzystów, zawiera trasy, możliwość rywalizacji użytkowników aplikacji, porównywanie wyników itp.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali zgodę.

Od 2008 roku zgłaszane były także zbiory, w których wykorzystywana jest technologia WiFi. Wśród ok. 20 zgłoszonych zbiorów administratorzy danych osobowych oferują usługi HOTSPOT jako narzędzia pozwalające na udostępnianie łącza internetowego użytkownikom. Statystyki udostępniane właścicielom HotSpota pozwalają śledzić ruch w sieci, między innymi informują o użytkownikach (adresy MAC, IP, czas logowania, czas sesji, obciążenie łącza, aktywni użytkownicy, zakończone usługi). Punkty dostępy WiFi można wykorzystać jako źródło informacji geolokalizacyjnych, ponieważ bez przerwy zgłaszają one swoje istnienie.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1, 3 i 5 ustawy o ochronie danych osobowych.

Administratorami danych osobowych zgłaszającymi tego typu zbiory były również podmioty publiczne tj. gminy dla kategorii osób - użytkowników sieci WiFi. W tych przypadkach jako podstawę prawną wskazywano ustawę z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2016 r. poz. 446), ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489). W powyższych zbiorach zakres przetwarzanych danych ogranicza się wyłącznie do danych zwykłych.

W 2016 roku zgłoszono ok. 12 zbiorów prowadzonych przez administratorów danych oferujących usługę systemu monitorowania i zarządzania klientami operatorów

GSM, w tym automatyczne powiadamianie o wygasających umowach.

Zawsze, gdy urządzenie przenośne jest włączone, jest ono połączone z konkretną stacją bazową (anteną). Operator telekomunikacyjny stale rejestruje te połączenia. Każda stacja bazowa posiada niepowtarzalny numer indentyfikacyjny i jest zarejestrowana w konkretnej lokalizacji. Zarówno operator telekomunikacyjny, jak i wiele urządzeń przenośnych może korzystać z sygnałów pochodzących z pokrywających się sąsiadujących ze sobą stacji bazowych, aby ustalić położenia urządzenia przenośnego ze zwiększoną dokładnością.

Jako podstawę prawną przetwarzania danych osobowych administratorzy wskazali art. 23 ust. 1 pkt 1, 3 i 5 ustawy o ochronie danych osobowych.

Z uwagi na powyższe należy mieć na względzie, że zastosowanie innowacyjnych rozwiązań technicznych może znacząco ingerować w sferę prywatności osób, których dane dotyczą. Dlatego przy dokonywaniu merytorycznej oceny zgłoszeń zbiorów danych osobowych do rejestracji konieczna jest szczególnie wnikliwa analiza, dokonywana przez pryzmat konieczności wyważenia z jednej strony ochrony praw osób, których dane dotyczą, zaś z drugiej naturalnych konsekwencji rozwoju w dziedzinie techniki. Warto bowiem zauważyć, że usługi, które wydają się dalece ingerujące w prywatność, jednocześnie często przyczyniają się do zwiększenia komfortu życia ich użytkowników poprzez ułatwienie załatwiania bieżących spraw życia codziennego. Wszystkie te aspekty są brane pod uwagę w postępowaniu rejestracyjnym i mają wpływ na dokonanie rejestracji zbioru danych lub wydanie decyzji o odmowie rejestracji.

ZBIORY DANYCH PROWADZONE w ZWIĄZKU ZE SPRAWOWANIEM OPIEKI FARMACEUTYCZNEJ

W roku 2016 Departament Rejestracji zakończył kilka postępowań prowadzonych w związku ze zgłoszonymi do rejestracji zbiorami danych dokonanymi w związku ze sprawowaniem opieki farmaceutycznej na podstawie ustawy z dnia 19 kwietnia 1991 r. o izbach aptekarskich (Dz. U. z 2014 r., poz. 1429). Przy rozpatrywaniu tego typu spraw zasadnicze znaczenie ma ustalenie, czy planowany przez administratora proces przetwarzania danych będzie wypełniał ustawową definicję pojęcia „opieka farmaceutyczna", czy też nie. W związku z niejednolitą interpretacją tego pojęcia należało dokładnie ocenić stan faktyczny każdej z tych spraw. Nie w każdym przypadku przeprowadzone postępowania wyjaśniające dawały podstawę do wpisania zbioru danych prowadzonego w celu sprawowania opieki farmaceutycznej do ogólnokrajowego, jawnego rejestru zbiorów danych osobowych.

7.1.2. Postępowania rejestracyjne dotyczące przetwarzania danych osobowych przez podmioty z sektora publicznego

REALIZACJA PROGRAMU 500+

Wejście w życie nowych przepisów prawnych skutkuje zgłaszaniem do rejestracji nowych zbiorów tworzonych w celu realizacji zadań lub kompetencji wynikających z wprowadzanych regulacji. W dniu 1 kwietnia 2016 r. Weszła w życie ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. z 2016 r., poz. 195) i rozpoczęto realizację rządowego „Programu Rodzina 500+". Ustawa określa warunki nabywania prawa do świadczenia wychowawczego oraz zasady przyznawania i wypłacania tego świadczenia[189]. W sprawach nieuregulowanych w tej ustawie stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2016 r. poz. 23 z późn. Zm.). W przypadkach wskazanych w ustawie możliwe jest przeprowadzenie rodzinnego wywiadu środowiskowego, o którym mowa w ustawie z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2016 r. poz. 930 z późn. Zm.).

Zgodnie z ustawą o pomocy państwa w wychowywaniu dzieci, postępowanie w sprawie świadczenia wychowawczego prowadzi organ właściwy, którym jest wójt, burmistrz lub prezydent miasta, właściwy ze względu na miejsce zamieszkania osoby ubiegającej się o świadczenie wychowawcze lub otrzymującej świadczenie wychowawcze. Organ właściwy może, w formie pisemnej, 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, a także do wydawania w tych sprawach decyzji. Status administratora danych w zakresie prowadzenia postępowań w sprawie świadczenia wychowawczego przysługuje zatem gminie, a w przypadku udzielenia upoważnienia do prowadzenia tych postępowań i wydawania decyzji – ośrodkowi pomocy społecznej lub innej jednostce organizacyjnej gminy.

Ponadto, zgodnie z ustwą o pomocy państwa w wychowywaniu dzieci, Marszałek województwa właściwy ze względu na miejsce zamieszkania osoby ubiegającej się o świadczenie wychowawcze pełni funkcję instytucji właściwej w związku z udziałem Rzeczypospolitej Polskiej w koordynacji systemów zabezpieczenia społecznego w przypadku przemieszczania się osób w granicach Unii Europejskiej i Europejskiego Obszaru Gospodarczego oraz wydaje decyzje w sprawach świadczenia wychowawczego realizowanego w związku z koordynacją systemów zabezpieczenia społecznego. Marszałek województwa może, w formie pisemnej, upoważnić dyrektora, jego zastępcę lub innego pracownika regionalnego ośrodka polityki społecznej lub innego pracownika urzędu marszałkowskiego do załatwiania w jego imieniu spraw dotyczących realizacji

[189] Świadczenie wychowawcze przysługuje matce, ojcu, opiekunowi faktycznemu dziecka albo opiekunowi prawnemu dziecka (art. 4 ust. 2 ustawy o pomocy państwa w wychowywaniu dzieci).

świadczenia wychowawczego w ramach koordynacji systemów zabezpieczenia społecznego, a także do wydawania w tych sprawach decyzji. Administratorem danych jest więc co do zasady województwo, a w przypadku upoważnienia do prowadzenia postępowań i wydawania decyzji – regionalny ośrodek pomocy społecznej.

Minister właściwy do spraw rodziny tworzy rejestr centralny obejmujący informacje gromadzone na podstawie przepisów ustawy przez organy właściwe i samorządy województw podczas realizacji zadań w zakresie świadczenia wychowawczego. Minister Rodziny, Pracy i Polityki Społecznej zgłosił do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbiór danych o nazwie „ZBIÓR DANYCH DOTYCZĄCY POMOCY PAŃSTWA w WYCHOWYWANIU DZIECI", który został wpisany do jawnego, ogólnokrajowego rejestru zbiorów danych osobowych pod numerem 167408.

W 2016 r. administratorzy danych zgłosili do rejestracji Generalnemu Inspektorowi 2 050 zbiorów dotyczących realizacji rządowego „Programu Rodzina 500+". Do jawnego ogólnokrajowego rejestru zostało wpisanych 1 815 zbiorów, a w przypadku pozostałych zgłoszeń konieczne było skierowanie pisma do wnioskodawców.

Ponadto w kilkunastu przypadkach administratorzy oświadczyli w treści zgłoszeń, że w związku z realizacją programu nie są przetwarzane dane szczególnie chronione, o których mowa w art. 27 ustawy o ochronie danych osobowych. W takiej sytuacji, administratorzy danych, którzy powołali i zgłosili do rejestracji administratora bezpieczeństwa informacji, byli informowani, że zgłoszony przez nich zbiór nie podlega obowiązkowi zgłoszenia do rejestracji stosownie do treści art. 43 ust. 1a ustawy o ochronie danych osobowych, jednak jak wynika z treści ustawy o pomocy państwa w wychowywaniu dzieci, w określonych przypadkach do ustalenia prawa do świadczenia wychowawczego niezbędne jest przedłożenie m. in. orzeczenia o stopniu niepełnosprawności dziecka. Oznacza to, że w zbiorach mogą być przetwarzane dane dotyczące stanu zdrowia i orzeczenia inne niż o ukaraniu, a zatem tzw. dane szczególnie chronione. Podkreślenia wymaga, że w przypadku ich przetwarzania na administratorze danych spoczywa obowiązek zgłoszenia zbioru danych do rejestracji, niezależnie od faktu powołania i zgłoszenia do rejestracji administratora bezpieczeństwa informacji. Po otrzymaniu tych informacji wielu administratorów dokonało ponownych zgłoszeń, uwzględniających powyższe uwagi, w wyniku czego zbiory te zostały wpisane do ogólnokrajowego rejestru zbiorów danych osobowych.

Zdarzało się także, że zgłoszenia zbiorów danych składane były przez powiatowe centra pomocy rodzinie. W świetle przepisów ustawy o pomocy państwa w wychowywaniu dzieci brak jest podstaw do uznania, że podmioty te są administratorami danych.

WPŁYW ZMIAN PRZEPISÓW PRAWA na OBOWIĄZEK REJESTRACJI ZBIORÓW DANYCH

Zgodnie z wyrażoną w art. 6 ustawy Kodeks postępowania administracyjnego zasadą legalizmu organy administracji publicznej działają na podstawie przepisów prawa. Oznacza to, że przetwarzają dane osobowe na podstawie przepisów prawa, w związku z wykonywaniem zadań określonych tymi przepisami. Częste zmiany zachodzące w systemie prawa (utrata mocy obowiązującej aktów prawnych oraz wprowadzanie do porządku prawnego

nowych regulacji) mają bezpośrednie przełożenie na obowiązki administratorów danych wynikające z rozdziału 6 ustawy o ochronie danych osobowych. Zmiany te, w przeważającej większości, skutkują koniecznością zgłaszania nowych zbiorów do rejestracji, czy też składania przez administratorów wniosków o wykreślenie z ogólnokrajowego, jawnego rejestru zbiorów danych, dotychczas prowadzonych w oparciu o uchylane przepisy zbiorów danych i zgłoszenia do rejestracji zbiorów danych tworzonych na podstawie nowych aktów prawnych.

W związku z wejściem w życie w dniu 1 kwietnia 2015 r. **przepisów ustawy z dnia 15 stycznia 2015 r. o zmianie ustawy o Służbie Celnej, ustawy o urzędach i izbach skarbowych oraz niektórych innych ustaw** (Dz. U. z 2015 r. poz. 211) do Generalnego Inspektora Ochrony Danych Osobowych licznie wpływały wnioski o wykreślenie z rejestru zbiorów danych osobowych składane przez naczelników urzędów skarbowych oraz zgłoszenia do rejestracji nowych zbiorów danych, a także zgłoszenia aktualizacyjne (do zbiorów pierwotnie zgłoszonych przez naczelników urzędów skarbowych) składane przez dyrektorów izb skarbowych. Zdaniem wnioskodawców, w związku z wejściem w życie ww. przepisów, naczelnicy urzędów skarbowych utracili status administratorów danych zawartych w zbiorach danych zgłoszonych do rejestracji Generalnemu Inspektorowi, a nowymi administratorami danych są według nich dyrektorzy izb skarbowych.

Nowelizacja ustawy nie zakładała jednak likwidacji urzędów skarbowych, jak i zmian w aktualnej strukturze organów podatkowych i i II instancji. Zgodnie z art. 5 ust. 6 ustawy o urzędach i izbach skarbowych do zadań naczelników urzędów skarbowych nadal należy w szczególności:

- ustalanie lub określanie i pobór podatków oraz niepodatkowych należności budżetowych, jak również innych należności, na podstawie odrębnych przepisów, z wyjątkiem podatków i należności budżetowych, których ustalanie lub określanie i pobór należy do innych organów;
- rejestrowanie podatników oraz przyjmowanie deklaracji podatkowych;
- wykonywanie kontroli podatkowej;
- wykonywanie egzekucji administracyjnej należności pieniężnych.

Naczelnik urzędu skarbowego, jako organ podatkowy i instancji oraz organ egzekucyjny, w dalszym ciągu wykonuje zatem swoje zadania przy pomocy podlegających mu komórek merytorycznych tworzących urząd skarbowy, w którym pracę świadczą pracownicy izby skarbowej. W uzasadnieniu projektu ustawy nowelizującej przepisy ustawy o urzędach i izbach skarbowych podkreślono, że pozostawienie naczelnika urzędu skarbowego, jako organu podatkowego i instancji, zapewni, że proponowane zmiany nie będą naruszały konstytucyjnej zasady dwuinstancyjności postępowania.

Tym samym naczelnicy urzędów skarbowych nadal pozostają administratorami danych osobowych przetwarzanych w związku z realizacją ich zadań ustawowych, określonych ww. przepisami prawa. W tym zakresie zarówno wnioskowanie przez naczelników urzędów skarbowych o wykreślenie z rejestru zbiorów danych osobowych, a następnie zgłaszanie przez dyrektorów izb skarbowych nowych wniosków w przedmiocie zarejestrowania takich zbiorów, bądź wniosków o dokonanie zmian w uprzednio zarejestrowanych przez naczelników urzędów skarbowych zbiorach było nieuzasadnione. Powołując się na definicję administratora danych zawartą w art. 7 pkt

4 ustawy, GIODO wskazywał, że pojęcie decydowania o celach i środkach przetwarzania danych osobowych, w przypadku administratorów danych ze sfery prawa publicznego, należy interpretować w sposób szczególny, tj. przez pryzmat właściwych przepisów prawa określających realizowane przez nich zadania. Swoboda decyzyjna przysługująca tym podmiotom zarówno w zakresie celów jak i środków przetwarzania danych osobowych jest wyznaczona przez właściwe przepisy prawa określające realizowane przez nie zadania. W przypadku administratorów danych ze sfery prawa publicznego decydujące znaczenie ma więc rodzaj i charakter nadanych danemu podmiotowi przez prawo kompetencji z zakresu spraw publicznych oraz zadania wyznaczone temu podmiotowi.

Stanowisko Generalnego Inspektora jest aktualne również na gruncie ustawy z dnia 10 lipca 2015 r. o administracji podatkowej (Dz. U. z 2015 r. poz. 1269). W ocenie organu do spraw ochrony danych osobowych utworzenie Centralnego Rejestru Danych Podatkowych i przetwarzanie w nim danych osobowych objętych zbiorami danych prowadzonymi przez dyrektorów izb skarbowych i naczelników urzędów skarbowych nie wpływa na zmianę statusu tych podmiotów. Dyrektorzy izb skarbowych i naczelnicy urzędów skarbowych nadal będą realizować swoje zadania, decydując o celach i środkach przetwarzania danych. Nie ma przeszkód, aby dyrektorów izb skarbowych i naczelników urzędów skarbowych nadal uznawać za administratorów danych na poziomie lokalnym, w zakresie wynikającym z przepisów określających ich zadania, niezależnie od faktu, iż dane te gromadzone są również w rejestrze centralnym i na tym poziomie ich administratorem jest minister właściwy do spraw finansów publicznych.

Innym przykładem zmian w systemie prawa były przepisy meldunkowe. Zgodnie z ustawą z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych (Dz. U. z 2006 r. Nr 139, poz. 993 z późn. Zm.), która utraciła moc obowiązującą z dniem 1 marca 2015 r., wojewódzkie zbiory meldunkowe były prowadzone przez wojewodów, zaś gminne zbiory meldunkowe oraz gminne ewidencje wydanych i unieważnionych dowodów osobistych przez gminy. Uchylona ustawa została z dniem 1 marca 2015 r. Zastąpiona dwiema nowymi: ustawą z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2015 r., poz. 388) oraz ustawą z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2016 r., poz. 391). W związku z tym, że nowa ustawa o ewidencji ludności nie zawiera jakichkolwiek unormowań dotyczących sposobu postępowania z likwidowanymi wojewódzkimi zbiorami meldunkowymi, dane osobowe w nich zawarte powinny zostać usunięte, a zbiory danych zgłoszone do wykreślenia przez wojewodów. W odniesieniu do gminnych zbiorów meldunkowych ustawa ta nie zawiera specjalnych regulacji w przedmiocie ich przekształcenia w rejestry mieszkańców, stanowiąc jedynie, że dotychczasowe gminne zbiory meldunkowe stają się odpowiednio rejestrami mieszkańców i rejestrami zamieszkania cudzoziemców. Wobec takiej regulacji zachodzi konieczność usunięcia danych osobowych, które nie będą podlegały przeniesieniu (nie zostaną „zmigrowane") z gminnych zbiorów meldunkowych do rejestrów mieszkańców i rejestrów zamieszkania cudzoziemców, zgłoszenia przez gminy do wykreślenia z rejestru zbiorów danych osobowych gminnych zbiorów meldunkowych oraz zarejestrowania nowych zbiorów w postaci rejestrów mieszkańców i rejestrów zamieszkania cudzoziemców.

W odniesieniu do gminnych ewidencji wydanych i unieważnionych dowodów osobistych ustawodawca, w ustawie o dowodach osobistych, zdecydował o ich likwidacji, ponownie

nie wskazując na tryb postępowania z danymi w nich przetwarzanymi. W takiej sytuacji gminy powinny usunąć zgromadzone w nich dane, a następnie wnioskować o wykreślenie tych zbiorów.

NIEWŁAŚCIWE PRZYPISANIE STATUSU ADMINISTRATORA DANYCH

Jak wskazano powyżej, pojęcie decydowania o celach i środkach przetwarzania danych osobowych, w przypadku administratorów danych ze sfery prawa publicznego, należy interpretować w sposób szczególny, tj. przez pryzmat właściwych przepisów prawa określających realizowane przez nich zadania. Zdarzają się jednak przypadki, kiedy podmioty z sektora publicznego zgłaszają do rejestracji zbiory danych osobowych, niewłaściwie przypisując sobie status administratora danych w nich zgromadzonych.

Wojewoda Wielkopolski zgłosił do rejestracji zbiór danych osobowych o nazwie „ZDARZENIA MEDYCZNE". W treści zgłoszenia poinformował, że dane przetwarzane w przedmiotowym zbiorze dotyczą osób, które składają wnioski do Wojewódzkiej Komisji do spraw Orzekania o Zdarzeniach Medycznych w Poznaniu o ustalenie zdarzenia medycznego, a jako podstawę prowadzenia zbioru wskazał przepisy ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2016 r., poz. 186 z późn. Zm.). W złożonych wyjaśnieniach wojewoda poinformował, że w jego ocenie przysługuje mu status administratora danych osobowych gromadzonych w wyżej wskazanym zbiorze z uwagi na fakt, iż przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta nakładają na niego obowiązki w postaci powołania 14 spośród 16 członków wojewódzkiej komisji, ustalenia wysokości wynagrodzenia za udział w posiedzeniu członków składu orzekającego komisji, jak również zapewnienia jej siedziby w urzędzie wojewódzkim. Zdaniem GIODO nie są to jednak argumenty, które pozwalałyby na uznanie, iż wojewódzka komisja do spraw orzekania o zdarzeniach medycznych nie jest administratorem danych osób wnioskujących o ustalenie zdarzenia medycznego. Zgodnie z ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta wniosek o ustalenie zdarzenia medycznego, zwany dalej „wnioskiem", wnosi się do wojewódzkiej komisji do spraw orzekania o zdarzeniach medycznych właściwej ze względu na siedzibę szpitala, która po naradzie wydaje, w formie pisemnej, orzeczenie o zdarzeniu medycznym albo jego braku, wraz z uzasadnieniem. Z powołanego wyżej przepisu wynika, że wojewódzka komisja do spraw orzekania o zdarzeniach medycznych jest podmiotem decydującym o celach i środkach przetwarzania danych osób wnioskujących o ustalenie zdarzenia medycznego w zakresie, w jakim prowadzi postępowanie w przedmiocie ustalenia zdarzenia medycznego.

Należy w tym miejscu wskazać na korespondencję wymienioną przez Generalnego Inspektora Ochrony Danych Osobowych z Ministrem Zdrowia, która dotyczyła wątpliwości interpretacyjnych w kontekście uprawnień wojewody oraz wojewódzkich komisji do spraw orzekania o zdarzeniach medycznych do przetwarzania danych osobowych zawartych w dokumentacji prowadzonych postępowań o ustalenie zdarzenia medycznego. Minister Zdrowia stanął na stanowisku, że administratorem danych osób wnioskujących o ustalenie zdarzenia medycznego jest wyłącznie wojewódzka komisja do spraw orzekania o zdarzeniach medycznych, ponieważ decyduje w praktyce o głównym celu przetwarzania danych - wydaje decyzje - oraz jest zobowiązana do odpowiedniego zabezpieczenia danych. Zdaniem

Ministra Zdrowia fakt udostępniania przez wojewodę środków zabezpieczających pozostaje bez znaczenia, ponieważ wszelkie roszczenia, wynikające przykładowo z niezachowania poufności danych, kierowane są do komisji a nie wojewody. Przepisy jedynie w niewielkim stopniu nadają wojewodzie uprawnienie do przetwarzania danych, a mianowicie kompetencje wojewody ograniczają się wyłącznie do: powołania 14 spośród 16 członków wojewódzkiej komisji, zapewnienia jej siedziby w urzędzie wojewódzkim oraz przechowywania dokumentacji związanej z toczącym się postępowaniem. Ponadto Minister Zdrowia wskazała, że zagadnienia mające na celu ustanowienie wojewódzkich komisji do spraw orzekania o zdarzeniach medycznych administratorem danych zawartych w dokumentacji postępowań prowadzonych przez te komisje oraz upoważnienie wojewody do przetwarzania tej dokumentacji zostaną uwzględnione w toku prac nad nowelizacją ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

Z uwagi na powyższe Generalny Inspektor Ochrony Danych Osobowych podtrzymał swoje stanowisko, zgodnie z którym art. 67n ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta nadaje uprawnienia do bycia administratorem danych osobowych również wojewodzie ale tylko w zakresie przechowywania dokumentacji (oświadczeń o braku konfliktu interesów, protokołów oraz orzeczeń wraz z uzasadnieniem) związanej z toczącym się postępowaniem przed komisją.

Wojewódzcy, powiatowi i miejscy komendanci policji zgłosili do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych kilkadziesiąt zbiorów danych dotyczących systemów audiowizualnych paralizatorów „SAP". W treści zgłoszeń zamieszczane były przez poszczególnych administratorów danych zasadniczo różne informacje między innymi dotyczące podstawy prawnej upoważniającej administratora do przetwarzania danych, kategorii osób, których dane przetwarzane są w zbiorze, celu przetwarzania, czy zakresu pozyskiwanych do zbioru danych. Są to podstawowe elementy, w oparciu o które Generalny Inspektor, w postępowaniu rejestracyjnym, dokonuje oceny zamierzonych procesów przetwarzania danych z punktu widzenia przestrzegania zasad przetwarzania danych osobowych. Przed rozpatrzeniem zgłoszeń należało zatem uporządkować oświadczenia administratorów zarówno w zakresie stanu faktycznego, jak i prawnego, aby stwierdzić, czy zasady te nie zostały naruszone.

W ocenie GIODO szczególnej analizy wymagało określenie podstawy prawnej upoważniającej administratorów do przetwarzania danych w przedmiotowych zbiorach. W większości złożonych zgłoszeń, wśród celów przetwarzania danych, wskazano dokumentowanie zgodności z prawem podejmowanych czynności służbowych oraz wykorzystywanie nagrań podczas prowadzonych postępowań przygotowawczych, skargowych i dyscyplinarnych, a także do celów szkoleniowych.

W związku z powyższym GIODO opracował sygnalizację, w której zwrócił się do Komendanta Głównego Policji m.in. Wnikliwe przeanalizowanie obowiązujących przepisów określających zadania i uprawnienia policji, z punktu widzenia podstawy prawnej przetwarzania danych pochodzących z monitoringu audiowizualnego paralizatorów „SAP" w celach, na które powołują się komendanci policji w treści składanych zgłoszeń do rejestracji zbiorów danych osobowych. Odnosząc się do przekazanych uwag, Komendant Główny Policji poinformował Generalnego Inspektora o przesłaniu do Komendantów Wojewódzkich/Stołecznego Policji i Centralnego Biura Śledczego pisma, w którym wskazał podstawy prawne upoważniające administratora do

przetwarzania danych, kategorię osób, których dane są przetwarzane w zbiorze, cel przetwarzania i zakres pozyskiwanych do zbioru danych. Wraz z przedmiotowym pismem jednostki wojewódzkie Policji otrzymały instrukcje: użytkowania systemu audiowizualnego stanowiącego wyposażenie przedmiotów przeznaczonych do obezwładniania osób za pomocą energii elektrycznej oraz obsługi sytemu audiowizualnego stanowiącego wyposażenie przedmiotów przeznaczonych do obezwładniania osób za pomocą energii elektrycznej. W wyżej wymienionych dokumentach, w pierwszych punktach wskazano, że system „SAP", rejestrujący obraz i dźwięk zdarzeń związanych z użyciem / wykorzystaniem wymienionego środka przymusu bezpośredniego przez policjantów, można wykorzystywać wyłącznie podczas wykonywania czynności służbowych w miejscach publicznych, w ramach realizacji zadań ustawowych Policji. Ponadto Komendant Główny Policji poinformował, że w związku z pismem Generalnego Inspektora, ponownie polecono Komendantom Wojewódzkim/ Stołecznemu Policji i Komendantowi Centralnego Biura Śledczego Policji przeprowadzenie analizy i weryfikację dokumentacji zbiorów, ich dokumentów rejestrujących i ewentualne uzupełnienie zgłoszeń zbiorów, w których gromadzone są dane pochodzące z monitoringu wizualnego lub audiowizualnego.

Efektem powyższych działań były aktualizacje informacji zawartych w pierwotnie złożonych wnioskach rejestracyjnych, zawierające prawidłowe informacje odnośnie podstawy prawnej upoważniającej administratora do przetwarzania danych, kategorii osób, których dane dotyczą, celu przetwarzania i zakresu pozyskiwanych do zbioru danych. Należy też mieć na względzie, że dotychczas kilkuset komendantów policji zgłosiło do rejestracji Generalnemu Inspektorowi powołanie administratora bezpieczeństwa informacji. Zgodnie z art. 43 ust. 1a ustawy o ochronie danych osobowych, 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. W treści nadesłanych zgłoszeń administratorzy danych nie wskazali na gromadzenie w zbiorach dotyczących systemów audiowizualnych paralizatorów „SAP" danych szczególnie chronionych, zatem w takiej sytuacji administrator danych nie podlega obowiązkowi notyfikacyjnemu względem Generalnego Inspektora, jednakże zbiór taki powinien zostać wpisany do rejestru zbiorów danych osobowych prowadzonego przez administratora bezpieczeństwa informacji u administratora danych, natomiast treść wpisu powinna uwzględniać wskazówki Generalnego Inspektora Ochrony Danych Osobowych.

ODMOWA REJESTRACJI ZGŁOSZONEGO ZBIORU

Zgodnie z art. 44 ust. 1 ustawy o ochronie danych osobowych Generalny Inspektor 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, ujęta w art. 26 ust. 1 pkt 3 ustawy, zasada adekwatności oznaczająca, iż 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. Równo-

waga jest zachowana wówczas, gdy administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu ich przetwarzania.

Gmina Konstancin-Jeziorna zgłosiła do rejestracji zbiór danych o nazwie <<EWIDENCJA UCZESTNIKÓW PROJEKTU "KONSTANCIN-JEZIORNA - GMINA BEZ WYKLUCZENIA CYFROWEGO">>. W treści zgłoszenia wnioskodawca oświadczył, że w przedmiotowym zbiorze przetwarza między innymi dane w postaci wizerunku beneficjenta w celu prowadzenia procesu rekrutacji do projektu „KONSTANCIN-JEZIORNA - GMINA BEZ WYKLUCZENIA CYFROWEGO" oraz jego realizacji. Wnioskodawca oświadczył, że wizerunki beneficjentów ostatecznych projektu były pozyskiwane na etapie uruchamiania projektu i na etapie rekrutacji w postaci kserokopii dowodów osobistych. Ponadto poinformował, że celem weryfikacji zameldowania na terenie Gminy Konstancin-Jeziorna osoby ubiegające się o udział w projekcie zobowiązane były do załączenia do formularza zgłoszeniowego kserokopii dowodu osobistego lub ewentualnie zaświadczenia o zameldowaniu. W związku z powyższym GIODO zwrócił się o uzasadnienie konieczności przetwarzania w zgłoszonym do rejestracji zbiorze wszystkich danych zawartych w kserokopii dowodu osobistego w celu, dla realizacji którego prowadzony jest ten zbiór. Administrator danych nie uzasadnił konieczności przetwarzania poszczególnych danych znajdujących się w dowodzie osobistym. Poinformował, że wizerunek i pozostałe dane pozyskane w postaci kserokopii dowodu osobistego umożliwiły weryfikację, czy osoba zgłaszająca się do projektu jest rzeczywiście tą osobą, za którą się podaje. Wnioskodawca argumentował ponadto, że Gmina zakupiła sprzęt komputerowy użyczony uczestnikom projektu z dotacji UE i budżetu państwa, ponosi za niego odpowiedzialność materialną, zatem weryfikacja uczestników projektu na podstawie danych zawartych w dowodzie osobistym jest kluczowym elementem zapewniającym wnioskodawcy bezpieczeństwo transakcji.

Generalny Inspektor Ochrony Danych Osobowych rozstrzygając sprawę podkreślił w pierwszej kolejności, że w żadnym przypadku nie jest dopuszczalne przyjęcie rozwiązań, które prowadzą do pozyskiwania danych osobowych w nieuzasadnionym zakresie, a więc z naruszeniem przywołanej powyżej zasady adekwatności. Praktyka polegająca na gromadzeniu kserokopii dowodów osobistych w celu identyfikacji osób uczestniczących w projekcie, w tym weryfikacji zameldowania na terenie gminy, powoduje, że do zbioru pozyskiwane są wszystkie dane osobowe zawarte w przedłożonych przez uczestników dowodach osobistych, w tym również te wykraczające poza zakres danych niezbędnych do identyfikacji osoby (np. nazwisko rodowe, imiona rodziców, wzrost, kolor oczu). W ocenie Generalnego Inspektora do identyfikacji osób uczestniczących
w projekcie wystarczające jest okazanie dowodu osobistego, porównanie danych zawartych w formularzu zgłoszeniowym z danymi w dowodzie osobistym i odpowiednie udokumentowanie tego wglądu, nie ma natomiast potrzeby pozyskiwania i przechowywania wszystkich danych osobowych zawartych w kopiach takich dokumentów. Pozyskiwanie wszystkich danych osobowych zawartych w kopiach dowodów osobistych (takich jak np. nazwisko rodowe, imiona rodziców, wzrost, kolor oczu) istotnie wykracza bowiem poza rzeczywiste potrzeby wynikające z celu przetwarzania danych w powyższym zbiorze, co stanowi naruszenie zasady adekwatności, o której mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

W konsekwencji Generalny Inspektor wydał decyzję, w której odmówił Gminie Konstancin-Jeziorna rejestracji zbioru danych osobowych o nazwie <<EWIDENCJA UCZESTNIKÓW PROJEKTU "KONSTANCIN-JEZIORNA - GMINA BEZ WYKLUCZENIA CYFROWEGO">>
i nakazał wnioskodawcy usunięcie z przedmiotowego zbioru danych osobowych nieadekwatnych do celu ich przetwarzania, tj. danych zawartych w kopiach dowodów osobistych 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.

Przedmiotowy zbiór danych został wpisany do ogólnokrajowego, jawnego rejestru danych osobowych w wyniku ponownego zgłoszenia zbioru danych, po usunięciu wad, które były powodem odmowy rejestracji tego zbioru.

7.2. Rejestracja Administratorów Bezpieczeństwa Informacji (ABI)

Z końcem 2016 upłynęły 2 lata odkąd funkcjonuje ogólnokrajowy, jawny rejestr administratorów bezpieczeństwa informacji prowadzony przez GIODO wprowadzony do ustawy o ochronie danych osobowych ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014, poz. 1662). Od dwóch lat stosowane są również rozbudowane przepisy dotyczących administratorów bezpieczeństwa informacji (ABI), które przyznały tej kluczowe znaczenie w zapewnianiu przestrzegania przepisów o ochronie danych osobowych u administratorów danych, którzy powołali taką osobę w swoich jednostkach organizacyjnych.

Celem rejestracji ABI jest zachowanie kontroli Generalnego Inspektora nad powoływaniem ABI oraz późniejszym wykonywaniem przez niego zadań. Rejestracja ABI odgrywa też ważną rolę w procesie edukacji i samoweryfikacji administratorów danych. Jeżeli administrator danych decyduje się na powołanie ABI musi zapewnić mu wymagane prawem warunki funkcjonowania (warunek podległości bezpośrednio kierownikowi jednostki organizacyjnej oraz niezależne wykonywanie zadań) oraz oświadczyć, że ABI spełnia ustawowe rygory kwalifikacyjne m.in. posiada odpowiednia wiedzę w dziedzinie ochrony danych osobowych. Z tego powodu rejestracja ABI przyczynia się nie tylko do wzmocnienia pozycji i roli administratorów bezpieczeństwa informacji (ABI), ale też do podniesienia efektywności całego systemu ochrony danych osobowych w Polsce.

Jest to bardzo ważne zwłaszcza w kontekście przygotowań do stosowania nowych o ochronie danych osobowych oraz do pełnienia przez wielu obecnych ABI funkcji inspektora ochrony danych osobowych przewidzianej w RODO. Wprowadzone wspomnianą nowelizacją ustawy o ochronie danych osobowych rozwiązania polegające na określeniu zasad sprawowania wewnętrznej kontroli przez ABI oraz ustalenie wymogów, jakie mają spełniać osoby wykonujące tą funkcję miało na celu przygotowanie zarówno ABI, jak i administratorów danych do stosowania RODO. W okresie prac

na nowelizacją ustawy o ochronie danych znany był projekt RODO, wobec czego sposób uregulowania statusu i funkcji ABI w ustawie o ochronie danych osobowych w wielu aspektach jest zbliżony do rozwiązań przyjętych w RODO.

Inspektorzy ochrony danych będą zatem kontynuatorami obecnej funkcji ABI jako fachowego podmiotu wspierającego administratorów danych w zapewnieniu prowadzonego przez nich przetwarzania danych osobowych z przepisami prawa. Często podkreśla się, że dysponujący odpowiednią wiedzą i umiejętnościami inspektorzy mają odegrać kluczową rolę w zapewnieniu zgodności przetwarzania danych osobowych z nowymi unijnymi regulacjami prawnymi zwłaszcza w okresie przejściowym i pierwszych latach stosowania nowych przepisów.

W roku 2016 r. do Biura GIODO wpłynęło 8102 zgłoszeń powołania administratora bezpieczeństwa informacji.

W i kwartale 2016 roku takich zgłoszeń było 2213, w II kwartale 2237, w III kwartale 1816, w IV kwartale 1836). W porównaniu do roku 2015, w 2016 r. liczba zgłoszeń powołania administratora bezpieczeństwa spadła o 14767 wniosków.

Porównując lata 2015 i 2016 stwierdzić należy, że w drugim roku funkcjonowania ogólnopolskiego rejestru ABI zmalała liczba zgłoszeń obarczonych błędami lub brakami formalnymi. Do pozytywnej zmiany przyczyniła się głównie edukacja administratorów danych osobowych oraz administratorów bezpieczeństwa informacji. Korzystny wpływ na podniesienie świadomości administratorów danych miało m.in. pojawienie się na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych ABI-informatora oraz odpowiedzi na wpływające zapytania udzielane przez pracowników Departamentu Rejestracji. W związku z nowelizacją przepisów ustawy o ochronie danych osobowych i wdrożeniem realizacji nowego zadania Generalnego Inspektora Ochrony Danych Osobowych, Departament Rejestracji przygotował informacje dotyczące nowelizacji ustawy o ochronie danych osobowych w zakresie pytania o obowiązek zgłoszenia administratora bezpieczeństwa informacji do rejestracji, a także opracowanie zatytułowane „Rejestracja ABI krok po kroku". Wypracowano kolejne stanowiska i interpretacje Generalnego Inspektora związane z nowelizacją ustawy. Powyższe materiały weszły w skład nowego serwisu GIODO pod nazwą „ABI - Informator", który to serwis w połowie lutego 2016 roku został udostępniony na stronie internetowej Generalnego Inspektora. Zawiera on szczegółowe informacje dotyczące: powołania, rejestracji i zadań administratora bezpieczeństwa informacji, a także sprawdzenia dla Generalnego Inspektora, obszerny zbiór pytań i odpowiedzi oraz w przystępny sposób zapewnia dostęp do obowiązujących przepisów prawa w tym zakresie. Serwis wyposażono także w narzędzia komunikacji z odwiedzającymi służące do zbieranie od nich informacji zwrotnej. W pierwszym roku funkcjonowania serwisu odnotowano oglądalność na poziomie 5-6 tysięcy odwiedzin miesięcznie.

W 2016 roku kontynuowano również cykl szkoleń oraz konferencji dotyczących zmian w ustawie o ochronie danych osobowych wprowadzonych ustawą o ułatwieniu wykonywania działalności gospodarczej

oraz wejściem w życie przepisów ogólnego rozporządzenia o ochronie danych osobowych. Szkolenia i konferencje miały na celu podniesienie świadomości ich uczestników w zakresie ochrony danych osobowych, powoływania administratorów bezpieczeństwa informacji, a w szczególności istoty oraz zakresu wykonywania zadań i obowiązków osób powołanych na tę funkcję i cieszyły się dużym zainteresowaniem ze strony osób, do których zostały skierowane.

Mimo tendencji spadkowej liczba zgłoszeń nieprawidłowych w 2016 r. nadal była dość duża. W obydwu latach funkcjonowania rejestru **do najczęściej popełnianych błędów w zakresie braków formalnych należały:**

- brak podpisu osoby uprawnionej do reprezentowania administratora danych,
- brak złożenia wymaganych oświadczeń przez administratora danych, że powołany administrator bezpieczeństwa informacji ma pełną zdolność do czynności prawnych, korzysta z pełni praw publicznych, posiada odpowiednią wiedzę w zakresie ochrony danych osobowych, podlega bezpośrednio kierownikowi jednostki organizacyjnej, bądź osobie fizycznej będącej administratorem danych;
- brak daty powołania administratora bezpieczeństwa informacji;
- brak innych wymaganych przepisami informacji dotyczących m. in. oznaczenia administratora danych osobowych, bądź oznaczenia administratora bezpieczeństwa informacji.

Wiele zgłoszeń dotkniętych było innymi niż braki formalne błędami, które uniemożliwiały zarejestrowanie powołania,

- zgłoszenie powołania więcej niż jednego administratora bezpieczeństwa informacji,
- zgłoszenie powołania zastępcy administratora bezpieczeństwa informacji,
- zgłoszenie powołania administratora bezpieczeństwa informacji, bez uprzedniego odwołania wcześniej zgłoszonego ABI.
- zgłoszenia, które nie zostały dokonane przed 30 czerwca 2015 r. Zawierające datę powołania administratora bezpieczeństwa informacji przed 1 stycznia 2015 r., w związku z czym zgodnie z art. 35 ustawy o ułatwieniu wykonywania działalności gospodarczej, administrator bezpieczeństwa informacji nie mógł zostać zarejestrowany, gdyż przestał pełnić swoją funkcję.
- zgłoszenia powołania na administratora bezpieczeństwa informacji osoby będącej kierownikiem jednostki organizacyjnej lub osoby fizycznej będącej administratorem danych lub osoby zarządzającej podmiotem posiadającym status administratora danych.

W zależności od rodzaju nieprawidłowości wnioskodawcy byli albo wzywani do usunięcia braków formalnych, albo - w przypadku innych błędów - informowani o warunkach zgodnego z prawem powołania i zgłoszenia administratora bezpieczeństwa informacji. Jednocześnie **przekazywana była informacja, że powołanie ABI jest uprawnieniem, a nie obowiązkiem administratora**.

Na skutek wezwań do usunięcia braków formalnych lub innych pism wskazujących nieprawidłowości w zgłoszeniu wielu administratorów danych przysyłało brakujące informacje lub prawidłowe zgłoszenia powołania ABI. Natomiast **część administratorów danych osobowych celowo nie odpowiadała na wezwania do uzupełnienia braków formalnych w zgłoszeniach,** ponieważ dzięki informacjom zawartym w ww. pismach uzyskali świadomość, że powołanie ABI nie jest obowiązkowe. Tym samym informowanie oraz wzywa-

nie do uzupełnienia braków formalnych administratorów danych, jest celowe nie tylko z punktu widzenia postępowania rejestracyjnego, lecz przyczynia się również do zwiększania świadomości administratora danych na temat statusu i znaczenia funkcji ABI. Jest to szczególnie ważne, ponieważ część rozwiązań z aktualnie obowiązującej ustawy o ochronie danych osobowych znajduje swoje odzwierciedlenie w przepisach ogólnego rozporządzenia o ochronie danych. Mowa tu m.in. o przepisach gwarantujących niezależność ABI (w przyszłości inspektora ochrony danych), a także o wymogu posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych.

W 2016 r. do ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych zostało wpisanych 5899 administratorów bezpieczeństwa informacji.

Administrator danych osobowych, który skorzystał z uprawnienia powołania administratora bezpieczeństwa informacji, mógł wystąpić z wnioskiem o wydanie zaświadczenia o zarejestrowaniu ABI (art. 46b ust. 4 ustawy o ochronie danych osobowych). Zgodnie z powołanym przepisem z takim wnioskiem mógł wystąpić również administrator bezpieczeństwa informacji. W **2016 roku zostało wydanych 574 zaświadczeń o zarejestrowaniu administratora bezpieczeństwa informacji. W** 98% przypadków wnioskodawcami byli administratorzy danych. Niestety również w zakresie wniosków o wydanie zaświadczenia zdarzały się błędy formalne, z których najczęściej popełnianym był brak załączenia dowodu uiszczenia opłaty skarbowej.

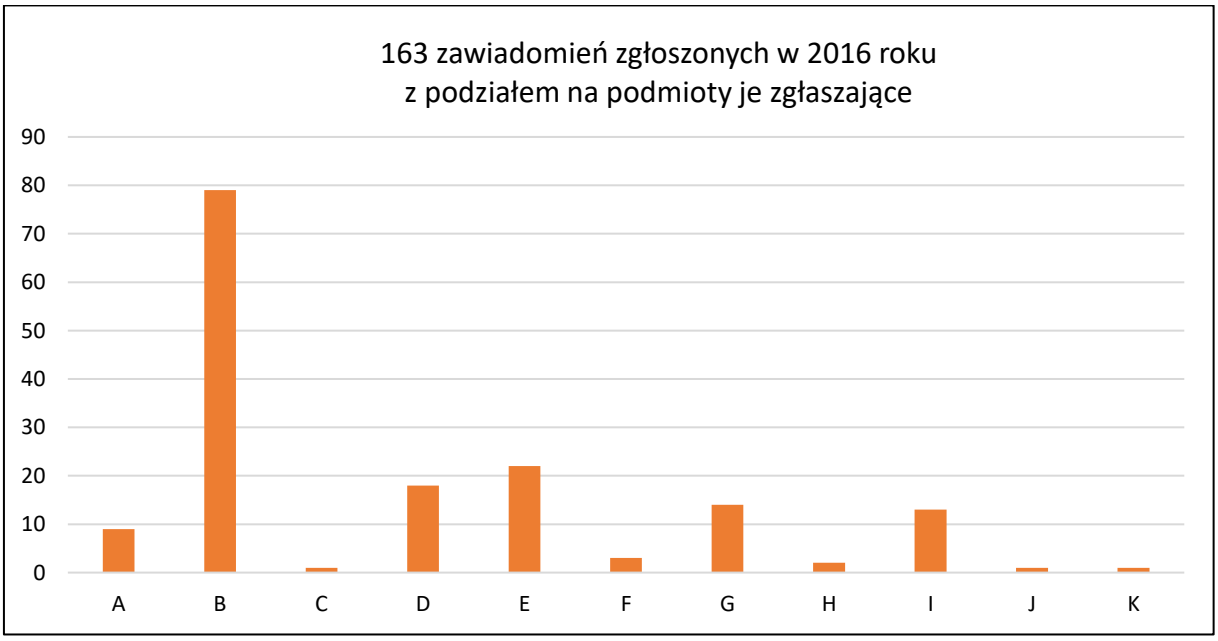
W 2016 roku zarejestrowano 1593 zgłoszeń odwołania ABI. Zgłoszenia odwołania stanowiły około ¼ wszystkich zgłoszeń, i liczba ta jest zdecydowanie większa w porównaniu do roku poprzedniego Wzrost liczby odwołań administratorów bezpieczeństwa informacji świadczyć może o wzroście świadomości administratorów danych osobowych odnośnie tego, że powołanie ABI jest uprawnieniem, a nie obowiązkiem administratora danych, oraz że powołanie jest możliwe jedynie wtedy, gdy osoba ta spełnia ustawowe warunki określone m.in. W art. 36a ust. 5 i 7 ustawy o ochronie danych osobowych. Jednym z podstawowych założeń nowelizacji ustawy o ochronie danych osobowych w zakresie rozbudowania przepisów o administratorze bezpieczeństwa informacji było bowiem, że do pełnienia tej funkcji wyznaczane być mogą jedynie osoby mające przede wszystkim określone merytoryczne przygotowanie oraz właściwe warunki pełnienia funkcji. Tylko powołanie takiej osoby może stanowić dla administratora danych realne fachowe wsparcie w zakresie nadzoru nad procesami przetwarzania danych osobowych oraz stanowić pomoc w zakresie wdrożenia obowiązków wynikających z ogólnego rozporządzenia o ochronie danych.

7.3. Zgłaszanie naruszeń ochrony danych

W świetle przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne przedsiębiorca telekomunikacyjny nie tylko musi chronić dane osobowe swoich klientów, ale także w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych zobowiązany jest w szczególności powiadomić o tym właściwy organ ds. ochrony danych osobowych (GIODO), a także abonenta lub użytkownika końcowego, którego dane zostały naruszone.

Przez naruszenie danych osobowych rozumie się przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych. Naruszenie danych osobowych powinno być zgłoszone niezwłocznie, ale nie później niż 24 godziny po wykryciu naruszenia.

W 2016 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęły 163 zawiadomienia o naruszeniu danych osobowych przez dostawców publicznie dostępnych usług telekomunikacyjnych.



Wykres 17. ***Podział zgłaszanych zawiadomień w 2016 roku o naruszeniu danych osobowych przez dostawców publicznie dostępnych usług telekomunikacyjnych wg poszczególnych podmiotów.***

W 2016 r. Zostały naruszone dane 1,7 mln abonentów lub użytkowników końcowych.

Analiza 2016 roku w kontekście danych z ostatnich lat (tabela poniżej) pokazuje rosnącą tendencję występowania naruszeń danych osobowych. Wynik prawie 1,7 mln abonentów , których dane zostały naruszone, zwłaszcza w kontekście poprzednich lat, pokazuje wyraźną wzrostową tendencję.

Lata:	2013	2014	2015	2016
Ilość podmiotów zgłaszających naruszenia (szt.)	14	16	10	11
Ilość zawiadomień (szt.)	136	155	93	163
Ilość abonentów lub użytkowników końcowych, których dane zostały naruszone w kolejnych latach (szt.)	217 893	29 395	68 722	1 698 386

Tabela 2. ***Dane statystyczne zgłaszanych zawiadomień w latach 2013-2016 o naruszeniu danych osobowych przez dostawców publicznie dostępnych usług telekomunikacyjnych.***

8. 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). 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.

Ogółem Generalny Inspektor Ochrony Danych Osobowych wydał w 2016 r. 11 decyzji administracyjnych dotyczących przekazania danych osobowych do państw trzecich.

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 w 2016 odnotowano spadek liczby wydanych decyzji dotyczących przekazywania danych osobowych do państw trzecich. Przeważająca większość prowadzonych przez Generalnego Inspektora postępo-

wań administracyjnych (9 decyzji) została prowadzona z uwzględnieniem rozstrzygnięcia organów ochrony danych osobowych z innych państw należących do Europejskiego Obszaru Gospodarczego, które uprzednio zaakceptowały dane WRK i zakończona wydaniem decyzji zatwierdzających WRK.

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.

TARCZA PRYWATNOŚCI (PRIVACY SHIELD)

Orzeczeniem z 6 października 2015 r. W sprawie Schrems (C-362/14) Trybunał Sprawiedliwości UE unieważnił decyzję Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r. W sprawie zapewniania przez podmioty z USA adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach "bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (notyfikowana jako dokument nr C(2000) 2441).

Tym samym transfery danych pomiędzy Europą a USA stanęły pod znakiem zapytania, a administratorzy danych musieli szukać innych przesłanek legalizujących transfer, jednocześnie czekając na kolejne porozumienie w sprawie przekazywania danych między tymi kontynentami.

W dniu 2 lutego 2016 r. Komisja Europejska i rząd Stanów Zjednoczonych osiągnęły porozumienie polityczne w sprawie nowych ram dotyczących transatlantyckich wymian danych osobowych w celach handlowych: Tarczy Prywatności UE-USA (IP/16/216). Natomiast 12 lipca 2016 Komisja Europejska przyjęła nową decyzję o adekwatności – decyzję wdrażającą umowę **Tarczy Prywatności (Privacy Shield)**, stwierdzając tym samym, że Stany Zjednoczone zapewniają odpowiedni poziom ochrony danych osobowych Europejczyków. Nowe ramy prawne mają w zamierzeniu zapewnić ochronę praw podstawowych obywatelom w UE, których dane osobowe są przekazywane do Stanów Zjednoczonych, jak również zapewnić jasność prawa przedsiębiorstwom, które muszą dokonywać transatlantyckich transferów danych.

Tarcza Prywatności jest mechanizmem samocertyfikowania dla przedsiębiorstw zlokalizowanych w Stanach Zjednoczonych. To ramy uznane przez Komisję Europejską za zapewniające odpowiedni poziom ochrony danych osobowych przekazywanych z podmiotu UE do przedsiębiorstwa z siedzibą w Stanach Zjednoczonych, a zatem jako element gwarancji prawnej dla takich operacji przekazywania danych.

Tarcza Prywatności dotyczy wszelkich danych osobowych przekazywanych z podmiotu UE do USA, w tym danych handlowych, stanu zdrowia lub związanych z zasobami ludzkimi

(danych HR), pod warunkiem że przedsiębiorstwo w USA będące odbiorcą dokonało samocertyfikacji zgodnie z ramami. Mechanizm ten polega na zobowiązaniu amerykańskich przedsiębiorstw do przestrzegania zasad, reguł i obowiązków określonych w ramach Tarczy Prywatności. Departament Handlu Stanów Zjednoczonych będzie prowadził regularne aktualizacje i przeglądy uczestniczących przedsiębiorstw w celu zapewnienia, by przestrzegały one zasad, którym się podporządkowały.

Umowa zawiera także wyraźne zabezpieczenia i wymogi przejrzystości regulujące dostęp administracji rządowej USA do danych osobowych, możliwość skorzystania ze środków odwoławczych wobec amerykańskich służb wywiadowczych za pośrednictwem urzędu Rzecznika w Departamencie Stanu oraz mechanizmy rozstrzygania sporów (z możliwością złożenia skargi do krajowych organów nadzorczych włącznie).

Tarcza Prywatności UE-USA obowiązuje w pełni od 1 sierpnia 2016 r. Ustalono także, że mechanizm będzie podlegał corocznym przeglądom.

9. Wystąpienia

Mocą art. 19a ustawy o ochronie danych osobowych, 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. 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. Podmiot, do którego zostało skierowane wystąpienie lub wniosek, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie w terminie 30 dni od daty jego otrzymania.

Generalny Inspektor Ochrony Danych Osobowych od lat obserwuje, iż wystąpienia kierowane na podstawie art. 19a ustawy o ochronie danych osobowych są skuteczną, „miękką" formą oddziaływania na administratorów danych. Większość podmiotów, do których zwraca się GIODO, uwzględnia przedstawiane w wystąpieniach sugestie, zmienia stosowane dotychczas praktyki czy też podejmuje współpracę z organem w celu wprowadzenia nowych przepisów, odpowiadających zasadom ochrony danych osobowych.

Zdecydowana większość wystąpień kierowana była w związku z rozpatrywanymi przez Generalnego Inspektora skargami oraz opiniowaniem projektów aktów prawnych. GIODO korzysta także z innych, mniej formalnych instrumentów oddziaływania na administratorów danych. Te różnego rodzaju wnioski i sygnalizacje mają na celu zwrócenie uwagi na zauważony przez GIODO problem jak również uzyskanie odpowiedzi w prowadzonej sprawie.

W roku 2016 łączna liczba wystąpień, sygnalizacji i wniosków przygotowanych przez GIODO wyniosła 109.

PUBLIKOWANIE DANYCH OSOBOWYCH w BIP I NA STRONACH INTERNETOWYCH

Dotychczas najczęstszym powodem kierowania przez Generalnego Inspektora wystąpień do podmiotów z sektora publicznego było nieprawidłowe realizowanie obowiązku udzielania informacji publicznej poprzez publikację na stronach internetowych uchwał jednostek

samorządu terytorialnego bez dokonania stosownej ich anonimizacji[190]. W obecnym roku sprawozdawczym stanowią one zdecydowaną mniejszość. Odnotować należy jednak fakt, że w wyniku przeprowadzonego postępowania z urzędu, skierowano wystąpienia do kilkunastu gmin i starostw w związku z publikacją uchwał bez usunięcia danych osobowych.

Generalny Inspektor skierował m.in. Wystąpienie do starostów i burmistrzów o podjęcie działań mających na celu zaprzestanie publikowania danych osobowych osób fizycznych zawartych w uchwałach w sytuacji, gdy jest to uzasadnione ochroną ich prywatności, oraz wyeliminowanie podobnych nieprawidłowości w przyszłości[191].

UDOSTĘPNIANIE DANYCH OSOBOWYCH W ZWIĄZKU Z REALIZACJĄ DOSTĘPU DO INFORMACJI PUBLICZNEJ

W związku z powtarzającą się praktyką stosowaną w gminach, polegającą na udostępnianiu danych osobowych osób fizycznych w związku z realizacją prawa dostępu do informacji publicznej, organ do spraw ochrony danych osobowych wystąpił także do Ministra Spraw Wewnętrznych i Administracji z wnioskiem[192] o podjęcia stosownych działań, mających na celu wskazanie wojewodom na zasadność zaniechania w gminach praktyki polegającej na umieszczaniu w uchwałach gminy pełnych danych osobowych osób fizycznych w przypadkach kiedy jest to zbędne oraz, jeżeli ich zamieszczanie jest konieczne - do dokonywania każdorazowej anonimizacji tych danych przed opublikowaniem uchwał na stronach internetowych.

GIODO wskazał, iż prawo do dostępu do informacji publicznej nie jest nieograniczone. 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. 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.

W związku z powyższym celem uzyskania wcześniej wskazanego balansu między prawem do informacji a prawem do ochrony danych osobowych, przed ewentualnym opublikowaniem dokumentu, powinien on zostać poddany zabiegowi **anonimizacji w** odniesieniu do danych osobowych osób fizycznych. Każda bowiem osoba fizyczna, której dane są przetwarzane przez m.in. organy administracji publicznej, korzysta z określonego w art. 5 ust. 2 omawianej ustawy ograniczenia w dostępie do informacji publicznej w postaci ochrony prawa do swojej prywatności, o ile z prawa tego wyraźnie nie zrezygnuje. Zamieszczanie w uchwałach rady gminy danych osobowych powinno następować tylko wtedy, kiedy jest to niezbędne. Publikowanie zaś na stronach internetowych uchwał rady gminy może odbywać się tylko po odpowiednim przetworzeniu (zanonimizowaniu) danych osobowych zawartych w tym dokumencie.

W odniesieniu do uchwały rady gminy, podjętej po rozpatrzeniu skargi osoby fizycznej, za-

[190] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. Z 2016 r. poz. 1764 ze zm.).
[191] M.in. pisma GIODO z dnia 16 czerwca 2016 r. o sygn. DOLiS-440-709/14/I/54513/16, DOLiS-440-709/14/I/54525/16, DOLiS-440-709/14/I/54528/16, DOLiS-440-709/14/I/54562/16.
[192] DOLIS-035- 2282/16.

wierającej jej dane osobowe w zakresie imienia oraz nazwiska, publikację uchwały powinno poprzedzać usunięcie tych danych.

Usunięcie danych osobowych musi być czynnością techniczną na tyle skuteczną, by dalsze operacje wykonywane na materiale stanowiącym informacje publiczną i czynienie z niego użytku, nie umożliwiało jakiegokolwiek dotarcia do danych osobowych, ich odtworzenia i odwrócenia procesu anonimizacji. Zatem w każdym przypadku udostępniania informacji publicznej w oparciu o przepisy ustawy o dostępie do informacji publicznej, konieczne jest uwzględnienie ograniczeń wynikających m.in. Z ochrony prywatności osoby fizycznej zapisanych w art. 5 niniejszej ustawy. Z normami z art. 5 ustawy o dostępie do informacji publicznej ściśle korespondują zasady adekwatności i celowości przetwarzania danych, które muszą być stosowane także we wszystkich tych sytuacjach, które dotyczą ewentualnego ujawnienia informacji.

GIODO wskazał również, iż zakres udostępnianych danych osób fizycznych może mieć wpływ na ponowne ich wykorzystywanie, gdyż ustawodawca przewidział szereg rozwiązań w tym zakresie w ustawie z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. 2016, poz.352), co może również rodzić ryzyko profilowania tj. automatycznej technice przetwarzania danych, polegającej na przypisaniu danej osobie „profilu" w celu przewidywania jej preferencji, zachowań, postaw.

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych skierował powyższe wystąpienie do każdego z szesnastu Wojewodów. Większość Wojewodów – odpowiadając już w roku 2017[193] - podzieliła zdanie Generalnego Inspektora i zapewniła, iż skieruje odpowiednie wytyczne do organów jednostek samorządu terytorialnego w celu przestrzegania przez nich zasad ochrony danych osobowych.

NIEDOZWOLONE PRZECHOWYWANIE DOKUMENTÓW TOŻSAMOŚCI

W innej ze spraw Generalny Inspektor zwrócił się do rektora jednego z uniwersytetów o wyeliminowanie przez uniwersytet praktyki **przechowywania w portierni domu studenckiego dowodów osobistych osób odwiedzających**, jako niezgodnej z przepisami ustawy o ochronie danych osobowych[194]. Ponadto wskazano, że zgodnie z ustawą o dowodach osobistych[195] zatrzymanie dowodu osobistego bez podstawy prawnej może stanowić wykroczenie.

Generalny Inspektor Ochrony Danych Osobowych skierował także wystąpienie do Polskiego Związku Piłki Nożnej[196] w związku z pozyskaniem informacji, iż przed rozgrywką

[193] Pismo Wojewody Warmińsko-Mazurskiego z dnia 21 kwietnia 2017 r. sygn.. PN.40.198.2017; Pismo Wojewody Wielkopolskiego z dnia 24 kwietnia 2017 r. sygn.. OA-XVII.132.5.2017.1; Pismo Wojewody Pomorskiego z dnia 19 kwietnia 2017 r. sygn.. PN-II.-20.16.2017.KG;Pismo Wojewody Lubuskiego z dnia 19 kwietnia 2017 r. sygn.. NK-I.40.21.2017.TDom; Pismo Wojewody Kujawsko-Pomorskiego z dnia 20 kwietnia 2017 r. sygn.. WNK.DT.IV.40.2.2017; Pismo Wojewody Pomorskiego z dnia 20 kwietnia 2017 r. sygn.. PN-II.020.16.2017;Pismo Wojewody Lubelskiego z dnia 20 kwietnia 2017 r. sygn.. PN-II.40.23.2017; Pismo Wojewody Podlaskiego z dnia 12 kwietnia 2017 r. sygn.. NK-II.40.26.2017.AK; Pismo Wojewody Dolnośląskiego z dnia 11 kwietnia 2017 r., sygn.. NK-N.40.43.2017.GD1; Pismo Wojewody Opolskiego z dnia 12 kwietnia 2017 r. sygn.. BOU.VIII.132.111.2017.IBP; Pismo Wojewody Podlaskiego z dnia 14 kwietnia 2017 r. sygn.. NK-II.40.26.2017.AK;Pismo Wojewody Zachodniopomorskiego z dnia 24 marca 2017 r., sygn.. P-1.002.17.2017.AB; Pismo Wojewody Wielkopolskiego z dnia 24 kwietnia 2017 r., sygn.. OA-XVII.132.5.2017.1;Pismo Wojewody łódzkiego z dnia 19 kwietnia 2017 r., sygn.. PNIK-I.4131.356.2017.

[194] Pismo GIODO z dnia 4 marca 2016 r. (DOLiS-440-2155/15/14712/17).

[195] Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (t.j. Dz. U. Z 2016 r. poz. 1948 ze zm.).

[196] Pismo z dnia 28 października 2016 r., syg. DOLiS-035-2286/16/SR.

piłkarską stosowana jest przez sędziów praktyka zatrzymywania i przechowywania dowodów osobistych zawodników w celu potwierdzenia ich tożsamości.

Informacje pozyskane przez organ do spraw ochrony danych osobowych wskazywały, iż zawodnicy nie mają możliwości sprzeciwienia się pozostawienia sędziemu dowodu osobistego, gdyż nie zostaną wtedy dopuszczeni do meczu. Jednocześnie nie są oni informowani w jakim celu dowód tożsamości ma zostać zatrzymany przez sędziego, jak i gdzie będzie w tym czasie przechowywany oraz w jaki sposób zabezpieczony przed osobami postronnymi. Natomiast w treści regulaminu rozgrywek piłkarskich zamieszczonego na stronie PZPN w art. 7 wskazano, iż dowód tożsamości ma zostać przedstawiony sędziemu, gdy ten ma wątpliwości co do tożsamości zawodnika biorącego udział w zawodach (a nie pozostawiony na czas meczu). Przyjęta, opisywana praktyka wykracza zatem poza regulacje regulaminu rozgrywek piłkarskich i prowadzi do bliżej nieokreślonego przetwarzania danych osobowych zawartych w dokumencie tożsamości w trakcie trwania meczu.

Przyjęte rozwiązania budzą zastrzeżenia w kontekście zasad wynikających z przepisów ustawy o ochronie danych osobowych w szczególności w aspekcie zasad przetwarzania danych osobowych (*art. 7 pkt 2 ustawy o ochronie danych osobowych*).

Przetwarzanie danych z dowodu osobistego nie będzie zatem niezgodne z prawem, jeśli przetwarzanie wszystkich danych pochodzących z tego dokumentu będzie znajdowało stosowną podstawę prawną, a zatem o ile nie będzie prowadziło do gromadzenia danych w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane są przetwarzane. Jednocześnie, co istotne, przetwarzanie danych nie może odbywać się w sposób, który narusza obowiązujące przepisy prawa.

GIODO wskazał, iż o ile sam sposób pozyskiwania danych osobowych jest z punktu widzenia ustawy o ochronie danych osobowych obojętny, to czynność przetrzymywania dokumentu tożsamości zawierającego w swej treści dane osobowe budzi uzasadnione zastrzeżenia organu pod kątem zgodności z podstawowymi zasadami przetwarzania danych osobowych: legalności, zasadności i celowości.

Ponadto organ przypominał, że nieuprawnione zatrzymanie dowodu tożsamości jest sprzeczne z przepisami ustawy z dnia 6 sierpnia 2010 roku o dowodach osobistych (*Dz. U. z 2016 r., poz. 391*), w której ustawodawca w art. 79 przewidział sankcje karne dla osób, które bez podstawy prawnej zatrzymują cudzy dowód osobisty. Przepisy karne powyższej ustawy tak naprawdę wyjaśniają „osobisty" charakter dokumentu, jakim jest dowód osobisty. Brak statusu podmiotu uprawnionego w rozumieniu ustawy o dowodach osobistych oznacza, iż zatrzymywanie dowodu (w sposób pozbawiający posiadania go przez posiadacza) staje się czynem karalnym.

W odpowiedzi na wystąpienie GIODO, pismem z dnia 29 listopada 2016 r. Prezes Polskiego Związku Piłki Nożnej[197] poinformował, iż zatrzymywanie dowodów osobistych zawodników nie stanowi rozwiązania systemowego przyjętego w ustanowionych przez Polski Związek Piłki Nożnej regułach organizacyjnych, sportowych i dyscyplinarnych. Zapewnił również, iż podjął szereg czynności mających na celu wyeliminowanie podobnych sytuacji w przyszłości.

[197] Sygn.. L.dz.221/2016/AB.

POZYSKIWANIE DANYCH PRZEZ KOMORNIKÓW

Proces przetwarzania danych osobowych przez komorników również rodził obiekcje skarżących. W wyniku jednej z nich Generalny Inspektor skierował wystąpienie do prezesa sądu rejonowego o zasygnalizowanie komornikom działającym na obszarze właściwości sądu potrzeby uwzględnienia zasad przetwarzania danych osobowych zgodnie z ustawą o ochronie danych osobowych oraz potrzeby uprzedniej weryfikacji informacji o potencjalnych źródłach zaspokojenia roszczeń wierzycieli, tak aby nie dochodziło do pozyskiwania danych przez podmioty nie mające interesu prawnego lub faktycznego w otrzymywaniu takich informacji[198].

WYSYŁANIE ZAPROSZEŃ NA PROFILAKTYCZNE BADANIA MEDYCZNE

W roku ubiegłym Generalny Inspektor Ochrony Danych Osobowych zwrócił się również do Ministra Zdrowia o rozważenie przeprowadzenia prac legislacyjnych mających na celu uregulowanie kwestii przetwarzania danych o stanie zdrowia w związku z prowadzeniem profilaktyki zdrowotnej lub realizacją programów zdrowotnych albo programów polityki zdrowotnej, w tym stworzenie właściwych podstaw prawnych funkcjonowania Systemu Informatycznego Monitorowania Profilaktyki[199].

Rozumiejąc społeczne znaczenie realizowanych przez Ministerstwo Zdrowia zadań w zakresie profilaktyki zdrowotnej i popierając inicjatywy mające na celu zachęcenie do udziału w badaniach profilaktycznych, Generalny Inspektor Ochrony Danych Osobowych zauważył pilną potrzebę stworzenia ku temu odpowiednich podstaw prawnych, sygnalizowaną już w wcześniej w korespondencji kierowanej do Ministra Zdrowia.

Braki w obowiązujących przepisach uwidoczniły się w związku z **praktyką prowadzenia przez jednostki samorządu terytorialnego wysyłki imiennych zaproszeń na profilaktyczne badania cytologiczne i mammograficzne**. Tymczasem przepisy ustawy z dnia 1 lipca 2005 r. o ustanowieniu programu wieloletniego „Narodowy program zwalczania chorób nowotworowych" (Dz. U. z 2005 r. Nr 143, poz. 1200, z poźn. Zm.) nie regulowały tej kwestii w sposób szczegółowy. Uzasadnienie dla prowadzenia spersonalizowanej wysyłki zaproszeń i przetwarzania danych jednostkowych wynikało jedynie w sposób pośredni z tej regulacji oraz programów profilaktyki raka piersi oraz raka szyjki macicy. Również kolejny program, przyjęty w drodze uchwały Rady Ministrów z dnia 3 listopada 2015 r. W sprawie ustanowienia programu wieloletniego na lata 2016-2024 pod nazwą „Narodowy Program Zwalczania Chorób Nowotworowych" (M. P. Z 2015 r. poz. 1165), nie mógł stanowić podstawy prawnej do tego rodzaju działań.

W tym kontekście zasadniczą, wymagająca odpowiedniego uregulowania w przepisach kwestią było zagadnienie **ram prawnych i zasad funkcjonowania Systemu Informatycznego Monitorowania Profilaktyki (SIMP)**, w którym – zgodnie z informacjami przekazanymi przez Ministerstwo Zdrowia – zawarte są m. in. dane dotyczące badań cytologicznych mammograficznych każdej z kobiet objętych *Programem profilaktyki raka szyjki macicy oraz Programem profilaktyki raka piersi i* który

[198] Pismo GIODO z dnia 16 listopada 2016 r., (DOLiS-440-2045/14/I/99606/16).
[199] DOLiS-035-924/16.

do końca 2015 r. służył jako narzędzie do prowadzenia imiennej wysyłki zaproszeń na badania profilaktyczne. GIODO wskazał, iż tylko stworzenie odpowiednich ustawowych podstaw funkcjonowania SIMP – w postaci unormowań dotyczących katalogu danych przetwarzanych w SIMP, sposobu i źródeł zasilania SIMP, katalogu (albo kręgu) podmiotów mających uprawnienie do dostępu do SIMP, katalogu (albo kręgu) podmiotów, którym udostępniane są informacje (dane) zgromadzone w SIMP oraz zasad tego udostępniania, okresu przechowywania danych w SIMP – pomoże uniknąć wątpliwości jakie obecnie ujawniają się w praktyce, a związanych z możliwością udostępniania danych zgromadzonych w SIMP innym podmiotom, czy prowadzeniem wysyłki imiennych zaproszeń na badania profilaktyczne. Dotychczasowy brak prawidłowego i wyczerpującego uregulowania SIMP prowadził do traktowania go wyłącznie jako systemu informatycznego, nie zaś zbioru danych o stanie zdrowia (danych szczególnie chronionych), co nie było – w opinii organu do spraw ochrony danych osobowych – stanem prawidłowym.

Ministerstwo Zdrowia pozytywnie odniosło się do wystąpienia GIODO, a opisywana kwestia była również przedmiotem dyskusji podczas prac nad nowelizacją ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw.

NIEZGODNE Z PRAWEM POZYSKIWANIE ZGODY NA PRZETWARZANIE DANYCH

Pismem z dnia 26 września 2016 r.[200] Generalny Inspektor Ochrony Danych Osobowych skierował wystąpienie do jednego z banków w związku z powzięciem informacji na temat nieprawidłowości w procesie przetwarzania danych osobowych przez ten Bank. Z informacji powziętych przez GIODO wynikło, że w jednym z oddziałów Banku podczas aktualizacji danych, w celu potwierdzenia ich zgodności ze stanem faktycznym, klientowi przedłożono formularz – Informacja o kliencie – dane ogólne opatrzony klauzulą zgody na przetwarzanie danych osobowych, z automatycznie zaznaczonymi polami potwierdzającymi udzielenie zgody. W wystąpieniu GIODO wskazał na przepisy art. 23 ust 1 pkt 1-5 ustawy o ochronie danych osobowych. Podkreślił, iż za prawnie usprawiedliwiony cel, o którym mowa w ustawie uważa się w szczególności marketing bezpośredni własnych produktów lub usług administratora danych. Zatem realizacja tzw. marketingu własnego administratora danych może odbywać się na podstawie przepisu prawa bez odrębnej zgody osoby, której dane dotyczą. Jednocześnie konieczne jest uwzględnienie sprzeciwu wobec przetwarzaniu danych osobowych, o ile zostanie on złożony przez osobę zainteresowaną.

GIODO wskazał również, iż konieczne jest takie sformułowanie zgody jak i skonstruowanie formularza pod względem technicznym, by **do wyrażania zgody nie dochodziło w sposób automatyczny, by kwestia ta zależała od nieskrępowanego wyboru osoby, której dane mają być przetwarzane**. Dodał, iż automatyczne zaznaczenie pola „*Tak zgadzam się*" dokonywane bez woli osoby niewątpliwie narusza wyżej wymienione zasady i w rzeczywistości prowadzi do fałszowania oświadczeń klientów Banku.

W odpowiedzi na wystąpienie Generalnego Inspektora Bank pismem z dnia 8 września 2016 r.[201] poinformował, iż dokonał przeglądu pro-

[200] DOLiS-980/16.
[201] DOLIS-035-980/16.

cesu pozyskiwania od klientów zgód marketingowych oraz wprowadzania zmian w trakcie trwania stosunków umownych z danym klientem.

Pismem z dnia 5 sierpnia 2016 r.[202] GIODO wystosował wystąpienie do jednej z Agencji Płatniczych w związku z powzięciem informacji, iż w regulaminie korzystania z konta w systemie teleinformatycznym Agencji zamieszczona jest klauzula o następującej treści: *„Wyrażam zgodę na przetwarzanie moich danych osobowych zawartych we Wniosku, zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Z 2014 r. poz. 1182 z późn. Zm). Przyjmuję do wiadomości, że: a. Zebrane dane osobowe będą przechowywane i przetwarzane przez Agencję z siedzibą: (…), zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Z 2014 r. poz. 1182 z późn. Zm); b. przysługuje mi prawo wglądu do moich danych osobowych oraz do ich poprawiania. Oświadczam, że zapoznałem/-a, się i akceptuję warunki Regulaminu korzystania z konta w systemie teleinformatycznym Agencji."*

GIODO wskazał, iż praktyka ta budzi zastrzeżenia w kontekście zasad wynikających z przepisów ustawy o ochronie danych osobowych. Ustawa o ochronie danych osobowych nie wprowadza uniwersalnej klauzuli zgody na przetwarzanie danych osobowych. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi. Zgoda na przetwarzanie danych osobowych określonych w formularzu nie jest wyrażana w żadnym konkretnym celu, natomiast zgoda na sam proces przekazania danych, tego celu nie określa, gdyż pod pojęciem przetwarzania danych osobowych mieszczą się operacje na danych osobowych, a nie cele ich realizacji, powstaje zatem pytanie, czy w ogóle powinna być wymagana taka zgoda.

Przetwarzanie danych osobowych jest dopuszczalne m.in. Wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Jeśli wykorzystywanie danych służy realizacji uprawnienia lub obowiązku określonego w przepisach prawa, to nie jest potrzebne dodatkowo żądanie zgody osoby na wykorzystywanie danych, ani uzasadnianie, że przetwarzanie danych służy dobru publicznemu lub niezbędnym celom administratora danych. Żądanie zgody wówczas, gdy wykorzystywanie danych służy realizacji normy prawnej, wprowadza w błąd, a także sugeruje możliwość wyboru, podczas gdy przekazanie danych jest obowiązkiem, bez którego cel pozyskania danych nie mógłby zostać zrealizowany. Jeżeli zatem istnieje przepis prawa, który daje prawo lub obowiązek przetwarzania danych, to zgoda nie jest potrzebna, w jej miejscu natomiast powinno znaleźć się wyjaśnienie, jakie konkretne cele będzie realizować Agencja.

W sytuacji, gdy uzyskanie zgody na przetwarzanie danych osobowych przez administratora danych jest wymagane przepisami prawa, w klauzuli powinny znaleźć się informacje o których mowa w art. 24 ust. 1 ustawy.

W odpowiedzi na wystąpienie, pismem z dnia 30 września[203] Agencja poinformowała, iż dokonała zmiany zawartej w Regulaminie korzystania z konta w systemie teleinformatycznym Agencji klauzuli informacyjnej dotyczącej przetwarzania danych osobowych.

[202] DOLiS-035-1237/16.
[203] Sygn. P 1960-DKiB-WZBI.0162.19(2)2016.

UDOSTĘPNIANIE DANYCH OSOBOWYCH OSOBOM NIEUPOWAZNIONYM

Impulsem skierowania wystąpienia do jednej z Wspólnot Mieszkaniowych w Olsztynie[204] było powzięcie wiadomości przez Generalnego Inspektora Ochrony Danych Osobowych, na temat nieprawidłowości w procesie przetwarzania danych osobowych przez tę Wspólnotę polegającej na możliwości dostępu poprzez Internetową Kartotekę Mieszkańca służącą mieszkańcom Wspólnoty do rozliczania rachunków do danych osobowych poprzednich właścicieli mieszkania oraz historii uiszczania przez nich wpłat. Powołując się na przepisy ustawy o ochronie danych osobowych i kodeksu cywilnego organ poinformował, iż współwłaściciele dla prawidłowego zarządzania współwłasnością muszą znać dane osobowe pozostałych właścicieli. Nie jest natomiast legalne ujawnianie mieszkańcom przez Wspólnotę danych osobowych poprzednich mieszkańców, w tym przebiegu czy prawidłowości regulowania przez nich należności.

Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. GIODO zwrócił uwagę Wspólnoty na zasady adekwatności i celowości oraz merytorycznej poprawności oraz, iż dane osobowe powinny być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Podkreślił, iż po osiągnięciu celu dane powinny zostać usunięte o ile ich dalsze przetwarzanie nie jest dopuszczalne na podstawie stosownych przepisów prawa. Wspólnota może więc na podstawie właściwych przepisów przetwarzać dane poprzednich mieszkańców w celach np. archiwalnych, sprawozdawczych, podatkowych czy dochodzenia roszczeń, ale nie w celu udostępniania ich osobom nieuprawnionym. Wspólnota, w myśl zasady merytorycznej poprawności danych powinna usunąć dane archiwalne poprzednich mieszkańców ze zbioru udostępnionego w postaci przedmiotowej internetowej kartoteki. Dlatego też działania polegające na przetrzymywaniu danych osobowych w bazie „kartoteki mieszkańca" w sposób umożliwiający w nie wgląd osobom trzecim, jest sprzeczne z opisanymi wyżej zasadami.

Organ do spraw ochrony danych osobowych podkreślił, iż korzystając z nowoczesnych technologii należy sięgać po rozwiązania, które dadzą gwarancje zachowania bezpieczeństwa przetwarzanych danych osobowych. Administrator jest swobodny w ich wyborze, o ile operacje wykonywane na danych osobowych przebiegać będą zgodnie z obowiązującymi przepisami prawa. System informatyczny stworzony na potrzeby zarządzania nieruchomościami nie powinien być używany w sposób powodujący niezgodne z prawem przetwarzanie danych osobowych. Gromadzone informacje przetwarzane przez administratora danych powinny być na bieżąco, zgodnie z zasadą merytorycznej poprawności uaktualniane, archiwizowane i przetwarzane w sposób proporcjonalny i adekwatny.

W piśmie z dnia 16 listopada 2016 r.[205] Wspólnota poinformowała, iż program komputerowy „kartoteka mieszkańca" został poprawiony.

[204] DOLiS-035-1452/16.
[205] DOLIS-sygn. WM/R23-25/2193/2016.

DANE OBYWATELI PRZEKAZYWANE WRAZ Z PODPISAMI POD OBYWATELSKIMI PROJEKATMI USTAW

W związku z sygnałami wskazującymi na brak jednoznacznego uregulowania w przepisach prawa kwestii zabezpieczania danych osobowych przekazywanych przez obywateli wraz z podpisami pod obywatelskimi projektami inicjatywy ustawodawczej, GIODO pismem z dnia 14 grudnia 2016 r.[206] skierował wystąpienie do Ministra Spraw Wewnętrznych i Administracji.

Zgodnie z przepisami czynności związane z przygotowaniem projektu ustawy, jego rozpowszechnianiem, kampanią promocyjną, a także organizacją zbierania podpisów obywateli popierających projekt, wykonuje komitet inicjatywy ustawodawczej. Jeżeli pod projektem podpisze się wymagana liczba obywateli, trafia on wraz z załączonym wykazem obywateli popierających projekt do Marszałka Sejmu.

W przepisach nie zostało wskazane, kto odpowiada za ochronę danych osobowych zgromadzonych w toku zbierania podpisów, kto jest ich administratorem. W rozporządzeniu Prezesa Rady Ministrów z dnia 28 września 1999 r. W sprawie ustalenia wzoru wykazu obywateli, którzy udzielają poparcia projektowi ustawy stanowiącej przedmiot inicjatywy ustawodawczej (Dz.U. 1999.poz. 79, nr 893) ustalono wzór wykazu obywateli, którzy udzielają poparcia projektowi ustawy stanowiącej przedmiot inicjatywy ustawodawczej. Zgodnie z nim, obywatele popierający dany projekt wraz ze swoimi podpisami udostępniają następujące dane osobowe: imię i nazwisko, adres zamieszkania (miejscowość, ulica, nr domu, nr lokalu); numer ewidencyjny PESEL. Również w rozporządzeniu brak jest informacji o tym, kto odpowiada za zgromadzone w wykazie dane osobowe. Ustawa o wykonywaniu inicjatywy ustawodawczej przez obywateli powinna wskazywać na podmiot odpowiedzialny za przestrzeganie wyżej wymienionych zasad. Nie jest bowiem oczywiste, że to komitet ustawodawczy jest administratorem danych osobowych zgromadzonych w toku zbierania podpisów pod obywatelskim projektem inicjatywy ustawodawczej. Zakładając jednak, że tak jest, wątpliwości budzi kwestia, kto odpowiada za listy z podpisami zgromadzone przez komitet inicjatywy ustawodawczej od momentu przekazania ich Marszałkowi Sejmu albo w sytuacji, gdy komitet ulegnie rozwiązaniu.

Przepisy ustawy nie muszą wprost wskazywać, kto jest administratorem danych określonego zbioru danych, o ile będą określać cały proces inicjatywy ustawodawczej, by znane były jej poszczególne etapy i towarzyszący im proces przetwarzania danych osobowych osób popierających projekt. Ustawodawca powinien precyzować jakie są cele przetwarzania danych osobowych oraz sposoby ich wykorzystywania, tak by regulacja była wyczerpująca dla realizacji celów ustawy, ale i bezpieczeństwa danych, w szczególności, gdy inicjatywa nie kończy się skierowaniem jej do parlamentu.

Mając powyższe na uwadze, Generalny Inspektor Ochrony Danych Osobowych wystąpił do Ministra o podjęcie prac nad uchwaleniem stosownych przepisów prawa. Minister Spraw Wewnętrznych i Administracji przekazał, zgodnie z właściwością powyższe wystąpienie Ministrowi Cyfryzacji[207]. GIODO oczekuje zatem na stanowisko w tej sprawie. Jednocześnie w trakcie prac nad projektem ustawy o zmianie ustawy o samorządzie gminnym i niektórych innych ustaw na etapie prac par-

[206] DOLiS-035-2106/16.
[207] Pismo z dnia 25 stycznia 2017 r., sygn.. DP-WLM-028-419/2016/Ech.

lamentarnych GIODO wskazał, że w projektowanych aktach konieczne jest doprecyzowanie kto będzie odpowiadał za wykazy zawierające dane osobowe osób podpisujących się pod inicjatywą uchwałodawczą w gminach, powiatach i województwach[208]

PUBLIKACJA DANYCH OSOBOWYCH DZIECI

W opisywanym okresie sprawozdawczym Generalny Inspektor Ochrony Danych Osobowych pozyskał informację, o publikacji na stronie internetowej publicznej szkoły listy dzieci przyjętych do oddziału przedszkolnego, klasy pierwszej szkoły podstawowej i klasy pierwszej gimnazjum w postaci tabeli obejmującej imiona i nazwiska dzieci, adresy zamieszkania dzieci oraz daty ich urodzenia (daty urodzenia dzieci w wykazie dzieci przyjętych do klasy pierwszej szkoły podstawowej).

W tej sprawie Generalny Inspektor wystąpił[209] do tej publicznej szkoły wskazując, iż zasady podawania do publicznej wiadomości wyników postępowania rekrutacyjnego do danego publicznego przedszkola, publicznej innej formy wychowania przedszkolnego, publicznej szkoły, publicznej placówki, na zajęcia w publicznej placówce oświatowo-wychowawczej, na kształcenie ustawiczne w formach pozaszkolnych lub na kwalifikacyjny kurs zawodowy, określone są precyzyjnie przepisami ustawy z dnia 7 września 1991 r. o systemie oświaty (t.j. Dz. U. z 2015 r., poz. 2156 ze zm.). Przepisy te stanowią, iż wyniki postępowania rekrutacyjnego podaje się do publicznej wiadomości w formie listy kandydatów zakwalifikowanych i kandydatów niezakwalifikowanych, zawierającej imiona i nazwiska kandydatów oraz informację o zakwalifikowaniu albo niezakwalifikowaniu kandydata do danego publicznego przedszkola, publicznej innej formy wychowania przedszkolnego, publicznej szkoły, publicznej placówki, na zajęcia w publicznej placówce oświatowo-wychowawczej, na kształcenie ustawiczne w formach pozaszkolnych lub na kwalifikacyjny kurs zawodowy.

Upublicznianie danych osobowych prowadzi do zapoznania się z nimi nieograniczonego kręgu osób, w tym osób do tego nieuprawnionych. Jedyną podstawą prawną udostępniania informacji stanowiących listę dzieci przyjętych do oddziału przedszkolnego, klasy pierwszej szkoły podstawowej czy klasy pierwszej gimnazjum, regulującą jednocześnie zasady upublicznienia tej informacji i katalog danych osobowych, które mogą być upublicznione, są przepisy ustawy o systemie oświaty.

W udzielonej odpowiedzi Dyrektor Szkoły poinformował Generalnego Inspektora, że dane osobowe uczniów zostały usunięte ze strony internetowej szkoły, oraz podjęte zostały w placówce działania w celu dostosowania procesu przetwarzania danych osobowych do wymogów określonych w aktach prawnych (zaplanowano szkolenia dla wszystkich pracowników szkoły, przyjęto w placówce nową politykę bezpieczeństwa i instrukcję zarządzania oraz zobowiązano pracowników do bezwzględnego przestrzegania przepisów o ochronie danych osobowych.

[208] DOLIS-023-153/17.
[209] DOLiS-035-2590/16.

10. Zawiadomienia o podejrzeniu popełnienia przestępstwa

Przepisy ustawy o ochronie danych osobowych przewidują odpowiedzialność karną za naruszenie niektórych obowiązków wynikających z przepisów tej ustawy.

Wśród napotykanych nieprawidłowości wyróżnia się w szczególności niespełnianie obowiązku informacyjnego przez podmioty przetwarzające dane osobowe oraz udostępnianie danych osobowych osobom nieupoważnionym. Pomimo ugruntowanej linii orzeczniczej sądów administracyjnych oraz organu do spraw ochrony danych osobowych, powracającym problem jest również zamieszczanie danych osobowych w Biuletynie Informacji Publicznej.

W roku 2016 Generalny Inspektor Ochrony Danych Osobowych skierował do organów ścigania 36 zawiadomień o podejrzeniu popełnienia przestępstw przez osoby odpowiedzialne za przetwarzanie danych osobowych.

Najwięcej przypadków dotyczyło podejrzenia popełnienia przestępstwa przetwarzania danych bez podstawy prawnej, w tym w celach marketingowych (art. 49 ustawy) oraz udostępnienia danych osobowych bez podstawy prawnej (art. 51 ustawy). Ponadto odnotowano przypadki podejrzenia popełnienia przestępstwa naruszenia obowiązku prawidłowego zabezpieczenia danych osobowych (art. 52 ustawy) oraz niespełnienia obowiązku informacyjnego (art. 54 ustawy). W kilku przypadkach skierowano zawiadomienie o utrudnianiu kontroli (art. 54a ustawy) oraz niezgłoszeniu zbioru do rejestracji (art. 53 ustawy). Należy zauważyć, że większość zawiadomień dotyczyło podejrzenia popełnienia więcej niż jednego przestępstwa określonego w ustawie o ochronie danych osobowych.

NIEWŁAŚCIWE ZABEZPIECZENIE DANYCH OSOBOWYCH

Przykładowo, do Biura GIODO wpłynęło pismo wraz z dowodem wskazującym na dokonanie mailingu z uwidocznioną dla każdego odbiorcy listą adresatów, czym zdaniem Generalnego Inspektora wypełniono znamiona przestępstwa określonego w art. 51 ustawy o ochronie danych osobowych polegającego na udostępnieniu danych osobowych osobom nieupoważnionym i art. 52 polegającego na naruszeniu obowiązku zabezpieczenia danych osobowych[210]. Adres poczty elektronicznej, ze względu na to, że może prowadzić do bezpośredniej lub pośredniej identyfikacji osoby fizycznej może stanowić daną osobową. Każdy administrator winien zatem odpowiednio zabezpieczyć te dane przed udostępnieniem osobom trzecim. Ryzyko takie istnieje zwłaszcza w procesie kierowania masowych ofert

[210] Zawiadomienie GIODO z dnia 4 listopada 2016 r. (DOLiS/ZAW-33/16/96778).

marketingowych za pomocą list mailingowych. W przypadku wysyłania korespondencji do większej liczby adresatów w szczególności należy zadbać o to, aby dane osobowe adresatów zostały ukryte (np. poprzez zastosowanie w wiadomości e-mail pola UDW). W konsekwencji wniesienia przez GIODO zawiadomień o podejrzeniu popełnienia przestępstwa w powyższych sprawach postępowania umarzano bądź odmawiano wszczęcia dochodzenia. GIODO w każdym przypadku korzystał z środka odwoławczego i składał zażalenie. Niestety w rezultacie rozpatrzenia zażaleń, większość spraw ponownie umorzono. W opinii GIODO nie jest właściwym bagatelizowanie takich spraw. GIODO ma nadzieję, że rozwiązania przyjęte w RODO – takie jak administracyjne kary pieniężne, zgłaszanie naruszeń – będą skuteczniejsze. Przyjęcie takich rozwiązań w RODO wskazuje, że nie jest zasadnym łagodzenie w tym zakresie odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych.

Konsekwentne umarzanie przez organy ścigania postępowań dotyczących naruszeń ustawy o ochronie danych osobowych prowadzi do lekceważenia przez szereg podmiotów tychże przepisów.

NIESPEŁNIENIE OBOWIĄZKU INFORMACYJNEGO

Wśród napotykanych nieprawidłowości wyróżnia się w szczególności niespełnianie obowiązku informacyjnego przez podmioty przetwarzające dane osobowe. Jedno z zawiadomień dotyczyło spółki, która wprawdzie wypełniła wobec skarżącego obowiązek informacyjny z art. 33 ustawy o ochronie danych osobowych, jednakże nastąpiło to dopiero po roku od złożenia wniosku, czym uniemożliwiono skarżącemu realizację jego uprawnień w zakresie kontroli przetwarzania jego danych osobowych[211]. Artykuł 33 ust. 1 ustawy wskazuje ściśle określony termin 30 dni od dnia otrzymania wniosku na udzielenie stosownej odpowiedzi. Przepis ten wprawdzie nie wskazuje na następstwo niedochowania powyższego terminu, jednakże uporczywe uchylanie się lub nieuzasadniona zwłoka w jego spełnieniu, może potencjalnie rodzić odpowiedzialność karną na podstawie art. 54 ustawy. Z prowadzonych postępowań przez Generalnego Inspektora wynika, że aspekt terminowości spełniania obowiązku informacyjnego realizowanego na wniosek osoby, której dane dotyczą, jest często bagatelizowany przez podmioty przetwarzające dane, co objawia się przede wszystkim poprzez wskazane przekraczanie terminu przewidzianego w ustawie, czy wręcz spełnianiem go dopiero po interwencji GIODO.

UDOSTĘPNIANIE DANYCH OSOBOWYCH OSOBOM NIEUPOWAZNIONYM

Pomimo ugruntowanej linii orzeczniczej sądów administracyjnych oraz organu do spraw ochrony danych osobowych, powracającym problem jest również **zamieszczanie danych osobowych w Biuletynie Informacji Publicznej** przez jednostki samorządu terytorialnego. W prowadzonej sprawie skarżący wskazał, że na stronie BIP zostały udostępnione wyniki kontroli wraz z jego danymi osobowymi, w tym tzw. danymi wrażliwymi, o których mowa w art. 27 ust. ustawy[212]. W przedmiotowej sprawie nie zachodziła żadna z określonych w art. 23 oraz 27 ustawy przesłanek pozwalających na przetwarzanie danych w tym zakresie, w związku z czym zaszło podejrzenie popełnienia przestępstwa określonego

[211] Zawiadomienie GIODO z dnia 27 stycznia 2016 r. (DOLiS/ZAW-3/16/5250).
[212] Zawiadomienie GIODO z dnia 3 lutego 2016 r. (DOLiS/ZAW-7/16/6982).

w art. 51 ustawy. Udostępnienie dokumentu, który zawiera dane osobowe, powinno zatem nastąpić przy uwzględnieniu prawa do prywatności osoby fizycznej, której on dotyczy, tj. po odpowiednim przetworzeniu (anonimizacji) danych osobowych w nim zawartych.

GIODO skierował również zawiadomienie o podejrzeniu popełnienia przestępstwa popełnienia przez osoby odpowiedzialne za przetwarzanie danych osobowych w pacjentów placówki, których **dane osobowe zostały udostępnione na stronie internetowej w związku z publikacją ogłoszeń o udzielenie zamówienia publicznego** na przełomie lat 2012-2015, – przestępstw określonych w art. 51 ustawy o ochronie danych osobowych[213], oraz art. 49 ustawy o ochronie danych osobowych[214], polegającym na naruszeniu zaniechania przetwarzania danych osobowych gdy ich przetwarzanie jest niedopuszczalne albo jeżeli osoba przetwarzająca nie ma do tego uprawnienia.

W uzasadnieniu zawiadomienia GIODO wskazał, iż numery **PESEL pacjentów** to niewątpliwie dane osobowe, w kontekście zaś zamieszczonych ogłoszeń o udzieleniu zamówień publicznych na konkretne leki stanowią dane osobowe wrażliwe o których mowa w art. 27 ust.1 ustawy o ochronie danych osobowych. Obie informacje przedstawione łącznie: PESEL i nazwa leku, dają bowiem możliwość ustalenia jakie leki przyjmuje dana osoba, a co za tym idzie, na co choruje.

Administrator nie miał podstaw do upubliczniania na przestrzeni lat na stronach internatowych danych osobowych swoich pacjentów w ogłoszeniach o udzieleniu zamówienia publicznego. Działania te nie mogły się również opierać na przepisach ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz.U. 2015 poz. 2058), która stanowi, że udostepnieniu podlega informacja publiczna, w tym treść i postać dokumentów urzędowych (art.6 ust. 1 pkt 4), jednak przy ich zamieszczeniu na stronie internetowej BIP należy uwzględniać wskazane w tej ustawie ograniczenia. Zgodnie bowiem z jej art. 5 ust.2 prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. a zatem publikując w Biuletynie Informacji Publicznej (jak również na innych stronach internetowych dotyczących zamówień publicznych) informację o udzieleniu zamówienia publicznego wraz z danymi osobowymi osób fizycznych, należy brać pod uwagę unormowania powołanego art. 5 ust 2 ustawy o dostępie do informacji publicznej.

BRAK PODSTAWY PRAWNEJ DO PRZETWARZANIA DANYCH

Do złożenia zawiadomienia o możliwości popełnienia przestępstwa określonego w art. 49 ustawy doprowadziło również **uporczywe kierowanie przez spółkę oferty marketingowej** na adres poczty elektronicznej e-mail, **pomimo wielokrotnego zgłaszania sprzeciwu** przez skarżącego co do przetwarzania jego danych w takich celach oraz zapewnianiu spółki, że usunęła adres ze swojej bazy danych[215]. Okoliczności sprawy wskazywały na masowy charakter tego naruszenia. W trakcie postępowania ustalono również, że spółka nie legitymowała się podstawą prawną do przetwarzania danych osobowych.

[213] Przestępstwa polegające na udostępnieniu danych osobowych osobom nieupoważnionym.
[214] Przestępstwa polegające na naruszeniu zaniechania przetwarzania danych osobowych gdy ich przetwarzanie jest niedopuszczalne albo jeżeli osoba przetwarzająca nie ma do tego uprawnienia.
[215] Zawiadomienie GIODO z dnia 26 lipca 2016 r. (DOLiS/ZAW-24/16/66801).

Generalny Inspektor Ochrony Danych Osobowych skierował również kilka zawiadomień o podejrzeniu popełnienia przestępstwa[216] przeciwko pracodawcom przetwarzającym dane osobowe swoich pracowników poprzez **pobieranie od nich odcisków palców w celu ewidencjonowania ich czasu pracy**.

GIODO przedstawiał, iż zakres danych osobowych pracowników, jakich może żądać zatrudniający, określa art. 22^1 kodeksu pracy (Dz.U. Z 2016 r., poz.1666)[217]. Kodeks pracy w zakresie w nim nieuregulowanym odsyła do przepisów ustawy o ochronie danych osobowych. Przepisy tej ustawy określają m.in., na jakiej podstawie można legalnie przetwarzać dane osobowe, wymieniając zgodę osoby, której dane dotyczą, czy istnienie przepisu prawa, który zezwala na przetwarzanie danych osobowych w określonym celu (art. 23 ust. 1 ustawy). Jednak w przypadku pozyskiwania danych osobowych pracownika, innych niż wskazane wyżej, m.in. linii papilarnych, nie można powoływać się na zgodę osoby, której dane dotyczą, jako podstawę prawną do przetwarzania danych osobowych. Aby zgoda osoby mogła być uznana za podstawę legalizującą przetwarzanie danych osobowych musi być wyrażona w sposób dobrowolny. GIODO podkreślał, iż w relacji zachodzącej między pracodawcą a pracownikiem trudno jest mówić o takiej dobrowolności, gdyż brak jest tu równowagi podmiotowej (stosunek nadrzędności i podrzędności podmiotów), co często może sprzyjać wymuszeniu zgody[218]. a zatem jedyną podstawą do gromadzenia przez pracodawcę odcisków linii papilarnych pracowników może być przepis prawa. Skoro jednak nie ma regulacji zezwalających pracodawcom na żądanie od podwładnych danych biometrycznych to zarówno ich pozyskiwanie jak i ich dalsze przetwarzanie, nie znajdują podstawy prawnej.

Jako dodatkowy argument przemawiający za tym, że pracodawca nie może pobierać i przetwarzać odcisków linii papilarnych w celu rejestracji godzin ich przyjścia i wyjścia z zakładu pracy GIODO wskazywał stanowisko Grupy Roboczej art. 29[219], która uznała w dokumencie roboczym w sprawie biometrii z dnia 1 sierpnia 2003 r. – że ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Oznacza to, że przy wykorzystywaniu danych osobowych należy kierować się zasadą proporcjonalności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych[220]. Nie można zatem uznać, aby wykorzystywanie danych biometrycznych do kon-

[216] DOLIS/ZAW-25/16/73172 dot. DOLiS-35-2059/16/AG; DOLIS/ZAW-38/16/107618 dot. DOLiS-35-3127/16/AG; DOLIS/ZAW- 6 /16 dot. DOLiS-35-3915/15/MP.

[217] Są to imię (imiona) i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia. Pracodawca może żądać także numeru PESEL oraz innych informacji, w tym imion i nazwisk oraz dat urodzenia dzieci, jeżeli od ich podania zależy korzystanie przez pracownika ze szczególnych uprawnień. Innych danych pracodawca może żądać jedynie wówczas, gdy ich udostępnienie nakazują odrębne przepisy powszechne obowiązującego prawa.

[218] Takie stanowisko GIODO poparł także Naczelny Sąd Administracyjny w wyroku z dnia 1 grudnia 2009 r. o sygn. akt I OSK 249/09, stwierdzając że: „wyrażona na prośbę pracodawcy pisemna zgoda pracownika, na pobranie i przetworzenie jego danych osobowych, narusza prawa pracownika i swobodę wyrażenia przez niego woli. (…) Brak równowagi w relacji pracodawca pracownik stawia pod znakiem zapytania dobrowolność w wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22^1 Kodeksu pracy katalog danych, których pracodawca może żądać od pracownika".

[219] Grupa 29 to organu konsultacyjny, składający się z przedstawicieli organów ochrony danych osobowych obywateli państw członkowskich Unii Europejskiej, którego rolą jest czuwanie nad stosowaniem przez państwa członkowskie Dyrektywy nr 95/46/WE w sprawie ochrony danych osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych)

[220] Art. 26 ust.3 mówi, iż dane muszą być adekwatne w stosunku do celów, w jakich są przetwarzane.

troli czasu pracy pracowników było proporcjonalne do zamierzonego celu ich przetwarzania. Czas pracy można bowiem kontrolować za pośrednictwem innych środków, mniej ingerujących w czyjąś prywatność . Grupa Robocza art. 29, również w opinii nr 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych przyjętej w dniu 27 kwietnia 2012 r., uznała, że pracodawca musi zawsze dążyć do zastosowania środków w jak najmniejszym stopniu ingerujących w prywatność, wybierając w miarę możliwości proces, w ramach którego nie stosuje się danych biometrycznych. W przypadkach, w których można odpowiednio uzasadnić taką konieczność, podstawę prawną takiego przetwarzania mógłby stanowić uzasadniony interes administratora danych określony wart. 7 lit. f) dyrektywy 95/46/WE. Oznacza to, że mogą wystąpić przypadki, w których stosowanie systemów biometrycznych może leżeć w uzasadnionym interesie administratora danych. Przykładowo, jeżeli należy w sposób szczególny zapewnić bezpieczeństwo stref wysokiego ryzyka, stosując mechanizm umożliwiający dokładne sprawdzenie, czy dane osoby mają prawo dostęp do tych stref, zastosowanie systemu biometrycznego może leżeć w uzasadnionym interesie administratora danych. W przedstawionych w zawiadomieniach sprawach, zgodnie z zasadą ogólną nie można uznać, że wykorzystanie biometrii do celów ogólnych pracodawcy – jak wymogi bezpieczeństwa własności i osób fizycznych, czy weryfikacja czasu pracy – wynika z uzasadnionego interesu nadrzędnego względem interesów lub podstawowych praw i wolności osób, których dane dotyczą. Przetwarzanie danych biometrycznych może być uzasadnione jako konieczne narzędzie zabezpieczające własność lub osoby fizyczne, tylko jeżeli istnieją dowody oparte na obiektywnych i udokumentowanych okolicznościach na występowanie konkretnego znacznego ryzyka.

W związku, iż w powyższych sprawach nie wystąpiła żadna ze wskazanych w art. 23 ust. 1 pkt 1-5 ustawy o ochronie danych osobowych przesłanek dopuszczających przetwarzanie biometrycznych danych osobowych pracowników podmiotów co stanowi czyn zabroniony stypizowany w art. 49 ust. 1 ustawy o ochronie danych osobowych [221], dlatego uzasadnionym było w tych przypadkach wniesienie zawiadomień o podejrzeniu popełnienia przestępstwa.

UTRUDNIANIE WYKONYWANIA KONTROLI GIODO

W kilku sprawach Generalny Inspektor Ochrony Danych Osobowych skierował zawiadomienia o popełnieniu przestępstwa określonego w art. 54a ustawy, tj. udaremniania lub utrudniania wykonywania czynności kontrolnych przez inspektora, m.in. poprzez uporczywe ignorowanie wezwań do złożenia wyjaśnień w sprawie[222].

[221] Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo, do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
[222] Zawiadomienie GIODO z dnia 29 stycznia 2016 r. (DOLiS/ZAW-4/16/5714).

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA

Zgodnie z ustawą o ochronie danych osobowych, do zadań Generalnego Inspektora należy m.in. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych. GIODO, w związku z tym prowadzi różnorodną działalność edukacyjną, mającą za zadanie zwiększać wśród społeczeństwa świadomość potrzeby ochrony naszej prywatności oraz poziom wiedzy na temat ochrony danych osobowych w Polsce. Ochrona naszej prywatności staje się bowiem elementem niemal każdej dziedziny naszego życia – kiedy prowadzimy nasze konto na portalu społecznościowym, bierzemy kredyt w banku, załatwiamy jakąś sprawę w urzędzie czy wypożyczamy łyżwy. Nasze dane osobowe są niezbędne do realizacji wielu usług, stąd zwykło się mawiać, że stanowią „paliwo", czy też „ropę naftową" XXI wieku. Wiedza związana ze świadomym korzystaniem z naszej prywatności staje się więc w dzisiejszych czasach nieoceniona.

Stąd też GIODO angażuje się w wiele inicjatyw edukacyjnych, także tych skierowanych doi najmłodszych. Czego przykładem są kolejne edycje Programu edukacyjnego GIODO „Twoje dane – Twoja sprawa" skierowanego do szkół. Zamierzeniem programu jest budowanie świadomych i odpowiedzialnych postaw względem ochrony danych osobowych.

Podnosimy też wiedzę i umiejętności profesjonalistów, organizując szkolenia sektorowe z zakresu ochrony danych osobowych przeznaczone dla Administratorów Bezpieczeństwa Informacji. Szkolenia mają za zadanie ułatwić zrozumienie i skuteczne wdrożenie nowych zasad i obowiązków, które będą spoczywać na przyszłych Inspektorach Ochrony Danych już od 25 maja 2018 r., tzn. od daty stosowania rozporządzenia.

GIODO od lat współpracuje także z uczelniami wyższymi w zakresie ochrony danych osobowych, a efektem tej współpracy jest w wielu przypadkach powstanie studiów podyplomowych z zakresu ochrony danych osobowych.

Ogólne rozporządzenie o ochronie danych podkreśla jeszcze rolę GIODO w upowszechnianiu w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumienia tych zjawisk. Znaczenie działań edukacyjnych polskiego organu ochrony danych będzie więc jeszcze rosło – tak samo jak aktywność GIODO na tym polu.

1. Działalność edukacyjna

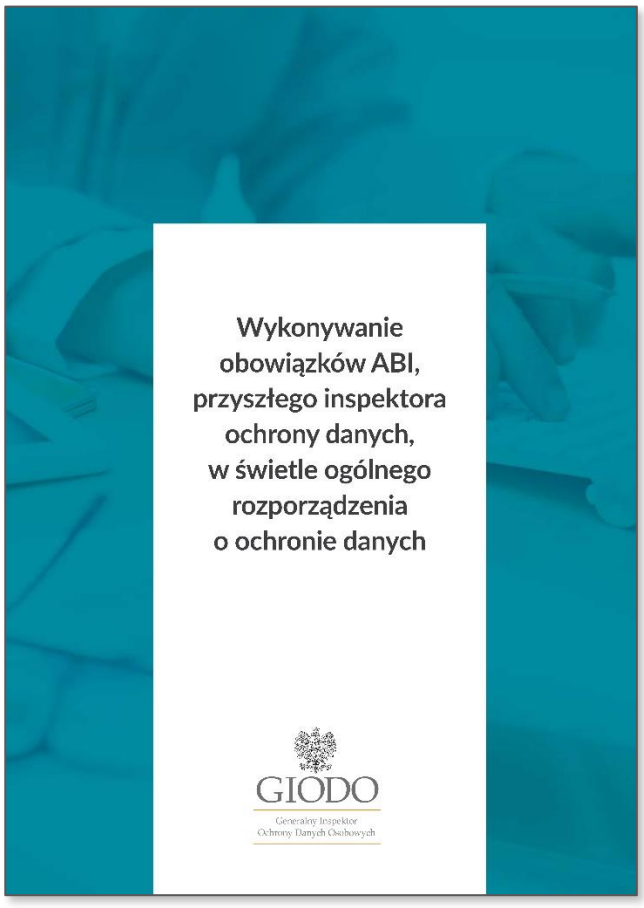
1.1. Publikacje

„POLSKA I EUROPEJSKA REFORMA OCHRONY DANYCH OSOBOWYCH”.

Publikacja ta powstała pod redakcją naukową dr Edyty Bielak-Jomaa i dr Dominika Lubasza. Jej autorami są przedstawiciele środowiska naukowego oraz praktycy zajmujący się od wielu lat zagadnieniami ochrony danych osobowych w Polsce i na świecie. W monografii zostały omówione istotne z praktycznego punktu widzenia zagadnienia dotyczące obowiązków prawnych administratora danych osobowych, a także kwestie związane z polską reformą ochrony danych osobowych przeprowadzoną w latach 2014 – 2015, w perspektywie bliskiego stosowania nowego unijnego prawa ochrony danych osobowych.

„WYKONYWANIE OBOWIĄZKÓW ABI, PRZYSZŁEGO INSPEKTORA OCHRONY DANYCH, W ŚWIETLE OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH”

Mając świadomość, że fachowa wiedza obecnych ABI – przyszłych inspektorów ochrony danych, przekładająca się na konkretne umiejętności praktyczne, jest fundamentem, na którym zbudować można w danej organizacji system skutecznej ochrony danych osobowych, GIODO pod koniec 2016 r. przygotował specjalną publikację **„Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych”**.



Zawiera ona podstawowe informacje, przydatne do lepszego poznania i zrozumienia roli i obowiązków przyszłego inspektora ochrony danych. Przedstawia bowiem istotę unijnej reformy prawa ochrony danych osobowych, w tym podstawowe pojęcia i zasady określone w rozporządzeniu ogólnym. Opisuje, jak w tym świetle oraz w kontekście nowych zadań administratorów danych kształtować się będzie wykonywanie obowiązków inspektora ochrony danych. Które z obowiązków związa-

nych z ochroną danych ciążą wyłącznie na administratorze, a w realizacji których wspierać może go inspektor ochrony danych.

W książce eksperci GIODO omawiają m.in.:

- na czym polega zmiana podejścia do ochrony danych osobowych,
- w jakim zakresie nastąpi wzmocnienie pozycji i niezależności inspektorów ochrony danych,
- kiedy obowiązkowo trzeba będzie przeprowadzać ocenę skutków planowanych operacji przetwarzania dla ochrony danych,
- jaki jest cel i istota uprzednich konsultacji z organem nadzorczym,
- jak prowadzić dokumentację przetwarzania danych osobowych zgodnie z przepisami rozporządzenia,
- jak przeprowadzić inwentaryzację danych osobowych,
- kiedy zgłaszać do GIODO przypadki naruszenia bezpieczeństwa danych,
- jaka odpowiedzialność grozi za przetwarzanie danych niezgodnie z prawem,
- jak jest praktyka i przyszłość sprawdzeń realizowanych przez ABI na zlecenie GIODO,
- gdzie szukać pomocnych informacji związanych z wykładnią nowych przepisów.

Publikacja ta dystrybuowana była m.in. jako dodatek do wybranych gazet, została też zamieszczona na stronie internetowej GIODO.

1.2. Szkolenia podmiotów zewnętrznych

W ramach prowadzonej działalności edukacyjnej w 2016 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 2016 r. Zwróciły się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o przeprowadzenie szkolenia znalazły się: Krajowa Rada Spółdzielcza, Wojewódzki Urząd Pomorski w Gdańsku, SKOK w Gdańsku, Starogardzki Klub Biznesu – Związek Pracodawców, Rzecznik Praw Dziecka, Uniwersytet Marii Curie-Skłodowskiej w Lublinie, Warszawski Uniwersytet Medyczny, Krajowa Szkoła Administracji Publicznej, Wyższa Szkoła Administracji i Biznesu w Gdyni, Stowarzyszenie Archiwistów Instytucji Wymiaru Sprawiedliwości – SAWS, Główny Urząd Statystyczny, Naczelna Rada Pielęgniarek i Położnych, Lubelski Urząd Wojewódzki, Ministerstwa: Spraw Zagranicznych (MSZ), Zdrowia (MZ), Sprawiedliwości (MS), Spraw Wewnętrznych i Administracji (MSWiA). Generalny Inspektor Ochrony Danych Osobowych i jego przedstawiciele przeprowadzili także szkolenia dla pracowników biur senatorskich Senatu RP, uczestników Ogólnopolskiego Dnia Praw Dziecka oraz dla dyrektorów Regionalnych Centrów Krwiodawstwa w Zawierciu.

Niektóre szkolenia miały cykliczny charakter, jak szkolenie realizowane w ramach VII edycji ogólnopolskiego programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli".

Ponadto w 2016 r. GIODO zainicjował cykl szkoleń dla administratorów bezpieczeństwa

informacji (ABI) wybranych sektorów. W analizowanym 2016 r. przeprowadzone zostały 2 szkolenia: dla ABI sektora publicznego (28.06.2016, 9.09.2016) oraz dla ABI z sektora szkolnictwa wyższego (24.11.2016).

W sumie w 2016 r. przeprowadzono 32 szkolenia podmiotów zewnętrznych.

1.3. Konkursy

W analizowanym 2016 r. Generalny Inspektor Ochrony Danych Osobowych był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

KONKURS NA ESEJ DOTYCZĄCY ZAGADNIEŃ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH.

Generalny Inspektor Ochrony Danych Osobowych po raz kolejny był organizatorem konkursu dla studentów kierunku prawo i administracja na esej dotyczący zagadnień z zakresu ochrony danych osobowych. Konkursy te mają na celu propagowanie wśród studentów polskich uczelni wiedzy z zakresu ochrony danych osobowych, umożliwienie im sprawdzenia swojej wiedzy w tej dziedzinie prawa, a także promowanie studentów posiadających umiejętność formułowania praktycznych rozwiązań w zetknięciu z problemami prawnymi. Przedmiotem VI edycji konkursu było przygotowanie eseju pt. „Przetwarzanie danych osobowych wykładowców uczelni na portalu służącym do oceny wykładowców". Uczestnicy konkursu mieli za zadanie rozwiązać kazus dotyczący przetwarzania danych o wykładowcach uczelni na portalu internetowym stworzonym przez studentów dla celów związanych z oceną wykładowców. Podczas rozwiązywania tego zadania konkursowego uczestnicy mieli okazję wykazać się wiedzą na temat tego, jak należy stosować przepisy polskiego prawa o ochronie danych osobowych do sytuacji opisanej w kazusie. 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.

KONKURS FOTOGRAFICZNY „DANE OSOBOWE na CO DZIEŃ" – OCHRONA DANYCH OSOBOWYCH W FOTOGRAFIACH WYKONANYCH PRZEZ 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 upowszechnienie wiedzy na temat prawa do prywatności i ochrony danych osobowych poprzez fotografie przedstawiające sytuacje życia codziennego, w których uczestniczą dzieci lub których mogą być świadkami – jak odebranie paczki od kuriera, wizyta u lekarza czy wypożyczenie roweru, które to czynności mogą

wiązać się z wykorzystaniem naszych danych osobowych.

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. Laureaci konkursu wraz z opiekunami wzięli udział w seminarium podsumowującym program edukacyjny w roku szkolnym 2015/2016, podczas którego wręczono nagrody.

„ZŁOTE PIÓRO PROGRAMU" - KONKURS DLA SZKÓŁ I OŚRODKÓW DOSKONALENIA NAUCZYCIELI

Już po raz czwarty 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 VI edycji programu. W konkursie udział wzięło 12 szkół i 1 ośrodek doskonalenia nauczycieli. Główną nagrodę – Złote Pióro Programu - otrzymało Publiczne Gimnazjum Nr 18 im. Prof. Jana Karskiego w Łodzi za inicjatywę edukacyjną – Gra planszowa-edukacyjna „Twoje dane – Twoja sprawa". Uroczystość wręczenia nagród odbyła się w dniu 7 czerwca 2016 r. podczas seminarium podsumowującego VI edycję programu.

NAGRODA GIODO ZA NAJLEPSZĄ PREZENTACJĘ W SESJI MŁODYCH MISTRZÓW FORUM TELEINFORMATYKI

Podczas XXII Forum Teleinformatyki, które odbywało się w dniach 29-30 września 2016 r. W Miedzeszynie, stałym punktem programu była sesja Forum Młodych Mistrzów, która w 2016 roku przebiegała pod hasłem „Ekonomiczne aspekty informatyzacji Państwa". Celem tego spotkania jest popularyzacja w środowisku młodych naukowców, ekonomicznych i prawnych zagadnień teleinformatyki w administracji publicznej. Udział w niej umożliwia studentom i młodym naukowcom zaprezentowanie szerokiemu gronu specjalistów informatyków i menadżerów sektora publicznego efektów swych badań naukowych i działań praktycznych. Generalny Inspektor Ochrony Danych Osobowych sprawuje patronat nad tym konkursem, przyznając nagrodę za najlepszą prezentację z zakresu ochrony danych osobowych. W Ministerstwie Cyfryzacji 12 grudnia 2016 r. odbyła się uroczystość wręczenia nagród Młodym Mistrzom Informatyki, którzy wygłaszali swoje prezentacje na XXII Forum Teleinformatyki. Nagrodę Główną przyznano za pracę z dziedziny ochrony danych osobowych, pt. „Profilowanie w oparciu o dane osobowe pochodzące z publicznych rejestrów medycznych. Analiza prawna z uwzględnieniem aspektów ekonomicznych".

1.4. Projekty i programy

W roku sprawozdawczym 2016, Biuro GIODO kontynuowało swój udział w różnego rodzaju projektach. Wśród nich wymienić należy projekt ARCADES, którego realizacja rozpoczęta się w 2014 r. Zakończyła się w 2016 r. oraz projekt PHAEDRA II. Programy te są finansowane ze środków Unii Europejskiej. Ponadto w 2016 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.

PROJEKT PHAEDRA II

W 2016 r. Biuro Generalnego Inspektora Ochrony Danych Osobowych kontynuowało 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 w ramach PHAEDRA II jest analiza czynników umożliwiających taką współpracę, z uwzględnieniem przepisów nowego prawa ochrony danych osobowych UE. Projekt PHAEDRA II skoncentruje się na analizie **trzech głównych obszarów zagadnień** istotnych dla europejskich organów ochrony danych osobowych: zapewnieniu spójności, wymianie różnych rodzajów informacji (włączając informacje niejawne) oraz koordynacji i współpracy w zakresie egzekwowania prawa.

Pierwsze spotkanie partnerów w ramach projektu odbyło się w poprzednim roku sprawozdawczym, tj. 20 stycznia 2015 r. W Brukseli[223].

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

[223] Szczegółowe informacje na temat projektu dostępne są na stronie internetowej http://www.phaedra-project.eu

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 rozwoju nowych technologii). W rezultacie opracowany został raport podsumowujący wyniki badań i prezentujący zasadnicze wnioski wynikające z przeprowadzonych analiz[224].

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.).

Podczas 108. Posiedzenia Grupy Roboczej Art. 29 ds. ochrony danych (Bruksela, 12-13.12.2016), przedstawiciel GIODO przedstawił informacje na temat wyników dotychczasowych prac prowadzonych w ramach projektu PHAEDRA II nad wypracowaniem mechanizmów efektywnej współpracy między organami ochrony danych i prywatności, szczególnie istotnych w kontekście wdrażania nowych unijnych przepisów o ochronie danych osobowych.

Czas trwania projektu wynosi 24 miesiące.

PROJEKT ARCADES

W 2016 r. Zakończyła się 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 było koordynatorem projektu, zaś partnerami byli: Vrije Universiteit Brussel z Belgii, Rzecznik Ochrony Danych Republiki Słowenii oraz Krajowy Urząd ds. Ochrony Danych i Wolności Informacji z Węgier.

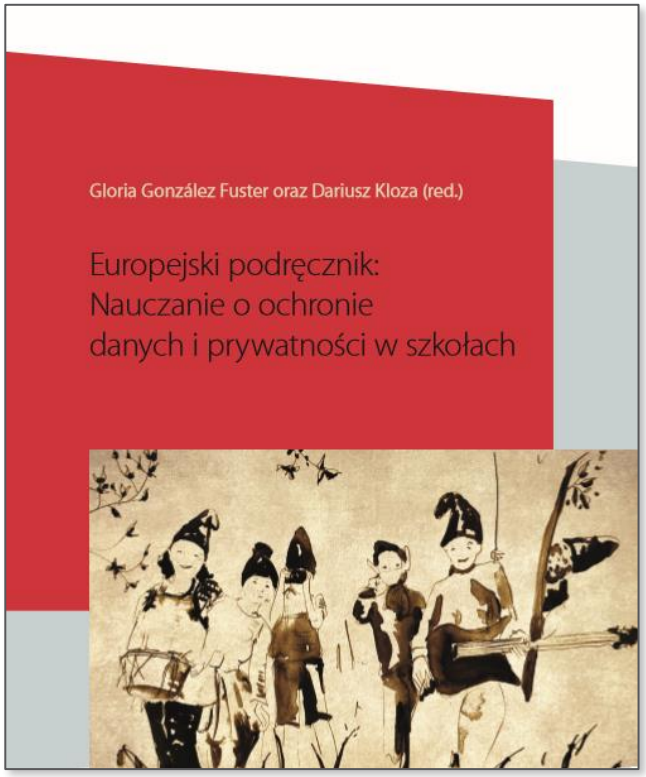
Inspiracją dla tego przedsięwzięcia był ogólnopolski program edukacyjny GIODO „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Generalny Inspektor podjął decyzję o przeniesieniu idei tego programu na grunt europejski. Celem projektu ARCADES było wprowadzenie do programu nauczania w szkołach państw Unii Europejskiej treści

[224] Raport dostępny jest na stronie internetowej projektu PHAEDRA http://www.phaedra-project.eu/?page_id=201

związanych z ochroną danych osobowych oraz prywatności. Adresatami projektu byli nauczyciele edukujący na poziomie podstawowym i średnim, których zadaniem było kształtowanie świadomych i odpowiedzialnych postaw wśród dzieci i młodzieży w wieku 6-19 lat. Pośród różnych działań zaplanowanych na czas trwania projektu, konsorcjum zapowiedziało 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 dniu 4 marca 2016 r. W Barcelonie odbyła się międzynarodowa konferencja podsumowująca ww. projekt. W konferencji uczestniczyli przedstawiciele szkół i instytucji edukacyjnych oraz organizacji społecznych, przedstawiciele organów ochrony danych z m.in. Z Polski, Węgier, Słowenii, Francji, Hiszpanii, Maroka, a także przedstawiciele Komisji Europejskiej, instytutów badawczych oraz szkół wyższych. W konferencji uczestniczyła grupa uczniów i nauczycieli z Gimnazjum nr 119 im. Marszałka Józefa Piłsudskiego w Warszawie, którzy zaprezentowali modelową lekcję języka angielskiego na temat ochrony danych osobowych, zatytułowany „Kto chce Twoje dane osobowe?". Lekcja ta otrzymała pierwszą nagrodę w konkursie na scenariusz lekcji z zakresu ochrony danych osobowych i prywatność, który GIODO zorganizował w ramach projektu ARCADES. Czas trwania projektu wynosił 18 miesięcy (3.XI.2014 r. – 3.05.2016 r.).

W 2015 r. W ramach projektu przygotowany został **Europejski poradnik. Nauczanie o ochronie danych i prywatności w szkołach,** którego polską wersję zaprezentowano w październiku 2016 roku podczas seminarium rozpoczynającego VI edycję Programu „Twoje dan e- twoja sprawa", zaś angielska wersja dostępna jest na stronie projektu ARCADES[225].



KRAJOWY PROGRAM EDUKACYJNY

W 2016 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

[225] http://arcades-project.eu/index.php/deliverables

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 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 roku szkolnym 2016/2017 w Programie edukacyjnym dla szkół z zakresu ochrony danych osobowych uczestniczyło 235 placówek oraz niemal 40 tys. uczniów. Przeszkolonych zaś zostało blisko 4 tysiące nauczycieli.

Inauguracja VII edycji Programu w roku 2016/2017 tradycyjnie już rozpoczęła się od dwudniowego seminarium szkoleniowego zorganizowanego przez Generalnego Inspektora Ochrony Danych Osobowych w dniach 25-26 października 2016 r. W szkoleniu tym udział wzięło **148 koordynatorów** wyznaczonych przez placówki biorące udział w Programie.

Dwudniowe szkolenie miało na celu przygotowanie uczestników Programu „Twoje dane – twoja sprawa (…)" do prowadzenia zajęć z uczniami w szkołach podstawowych, gimnazjach i szkołach podstawowych na temat ochrony danych osobowych i prawa do prywatności, jak również przedstawicieli ośrodków doskonalenia nauczycieli do prowadzenia spotkań z nauczycielami i dyrektorami szkół w ramach programu. Podczas szkolenia uczestnicy otrzymali pakiety edukacyjne 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 i przedstawiciele Komendy Głównej Policji.

Warsztaty były więc 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.

Pedagodzy, korzystając m.in. Ze szkoleń przeprowadzonych przez ekspertów z Biura

Generalnego Inspektora Ochrony Danych Osobowych i otrzymanych materiałów dydaktycznych, zrealizowali 3583 lekcje, podczas których poruszali treści związane z ochroną danych osobowych i prawem do prywatności. Najczęściej były to godziny wychowawcze, informatyka, lekcje polskiego lub języka obcego.

Program edukacyjny GIODO „Twoje dane – Twoja sprawa" to również setki zrealizowanych inicjatyw[226] - apeli, teleturniejów, gier planszowych, gier miejskich, konkursów, pikników, autorskich przedstawień, happeningów, spotkań, warsztatów czy pogadanek. Angażowały one nie tylko całą społeczność szkolną (uczniów, nauczycieli, rodziców i przedszkolaków), ale także środowisko lokalne (mieszkańców miast i liczne urzędy).

Te formy upowszechniania wiedzy i podnoszenia świadomości z zakresu ochrony danych osobowych niezmiennie cieszą się dużym uznaniem zarówno uczniów, jak i nauczycieli i innych osób w nich uczestniczących. Są bowiem uznawane przez realizujących Program nauczycieli za najbardziej skuteczne i atrakcyjne.

Seminarium podsumowujące VII edycję programu „Twoje dane - Twoja sprawa" odbyło się 6 czerwca 2017 r. W Pałacu Kultury i Nauki w Warszawie, z udziałem honorowych patronów Programu – Rzecznika Praw Dziecka oraz Ministerstwa Edukacji Narodowej, a także przedstawiciela Ministerstwa Spraw Wewnętrznych i Administracji oraz Przewodniczącego Krajowej Rady Radiofonii i Telewizji.

Podczas tego wydarzenia odbyło się uroczyste wręczenie nagród i wyróżnień w konkursach, które Generalny Inspektor Ochrony Danych Osobowych zorganizował w ramach VII edycji tego Programu.

ERASMUS+

GIODO realizuje także projekt „Współpraca na rzecz innowacji i wymiany dobrych praktyk w dziedzinie szkolnictwa wyższego" w ramach programu Erasmus+. Projekt ma na celu stworzenie innowacyjnego programu studiów podyplomowych w zakresie ochrony danych osobowych odpowiadającego na potrzeby rynku. Koordynatorem projektu jest Instytut Nauk Informatycznych i Technologii Św. Pawła Apostoła w Ochrydzie, zaś partnerami projektu są Generalny Inspektor Ochrony Danych Osobowych, Dyrektoriat Ochrony Danych Osobowych (Macedonia), Komisja Ochrony Danych Osobowych (Bułgaria) oraz Uniwersytet Łódzki. Realizacja projektu potrwa 28 miesięcy.

W dniu 19 lipca 2016 r. W Biurze GIODO odbyło się spotkanie związane z projektem. Podczas spotkania szczegółowej analizie poddana została przygotowana przez GIODO na potrzeby projektu analiza „Study on Labour Market Needs and Gaps in the Postgraduate Education Offer in the fields of IT Law, IT Security, Right to Privacy and Personal Data Protection".

[226] http://giodo.gov.pl/pl/1520272/9736

1.5. Konferencje, seminaria, spotkania

W roku sprawozdawczym 2016, 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.

X DZIEŃ OCHRONY DANYCH OSOBOWYCH, 28.01.2016

Zagrożenie prywatności w związku z gromadzeniem i przetwarzaniem wielkich zasobów danych i konieczność wypracowania rozwiązań, które przeciwdziałać będą nadużyciom w tym zakresie jest w chwili obecnej jednym z pilniejszych zadań stojących przed organem ds. ochrony danych osobowych. Dlatego zagadnienie to stało się tematem konferencji zorganizowanej przez GIODO wspólnie z Uniwersytetem Warszawskim z okazji X Dnia Ochrony Danych Osobowych (28.01.2016).

Święto to obchodzone jest co roku 28 stycznia – w rocznicę otwarcia do podpisu 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.

Wydarzenia związane z X 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. Ale w 2016 roku miały wyjątkowy charakter i formułę. GIODO bowiem zaprosił do współorganizacji obchodów tego święta uczelnie i szkoły wyższe, z którymi ma zawarte porozumienia o współpracy. Dlatego w poszczególnych ośrodkach akademickich odbywały się konferencje poświęcone różnym innym istotnym tematom związanym z szeroko pojętą problematyką ochrony prywatności i danych osobowych. Pierwsze z wydarzeń odbywało się już 13 stycznia 2016 r. na Uniwersytecie Śląskim w Katowicach. Była to konferencja nt. przetwarzania danych osobowych w sektorze służby zdrowia. GIODO wspólnie z Wyższą Szkołą Biznesu w Dąbrowie Górniczej zorganizował konferencję dotyczącą marketingu bezpośredniego (14.01.2016), zaś we współpracy z Wyższą Szkołą Policji w Szczytnie – Konferencję pt. „Kradzież Tożsamości" (19.01.2016). Natomiast główne obchody Dnia, tj. 28 stycznia 2016 r., odbywały się w Warszawie, gdzie GIODO wspólnie z Uniwersytetem Warszawskim zorganizował konferencję na temat Big Data. Kolejne wydarzenia z okazji X Dnia Ochrony Danych Osobowych miały miejsce w lutym w Akademii Leona Koźmińskiego w Warszawie, gdzie odbyła się

konferencja poświęcona nowej roli i pozycji administratorów bezpieczeństwa informacji (23.02.2016) oraz na Uniwersytecie Kardynała Stefana Wyszyńskiego, gdzie zorganizowana była konferencja na temat przetwarzania danych osobowych przez kościoły i związki wyznaniowe (25.02.2016). Do współorganizacji obchodów włączył się także Uniwersytet Łódzki, w którym 19 i 20 stycznia 2016 r. odbywały się warsztaty i porady prawne.

Szkoły i ośrodki doskonalenia nauczycieli współpracujące z Generalnym Inspektorem Ochrony Danych Osobowych w ramach Ogólnopolskiego Programu edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli", również aktywnie włączyły się w obchody X Dnia Ochrony Danych Osobowych, organizując wydarzenia podkreślające wagę ochrony prywatności i danych osobowych.

KONFERENCJA PT. „NOWA REGULACJA PRZETWARZANIA DANYCH OSOBOWYCH – SKUTKI w SEKTORZE BANKOWYM", WARSZAWA, 10.03.2016

Zwrócenie uwagi przedstawicieli polskiego sektora bankowego na problematykę ochrony danych osobowych w kontekście świadczonych usług bankowych w świetle reformy unijnego prawa ochrony danych, było głównym celem Konferencji zorganizowanej przez Związek Banków Polskich. Podczas tego wydarzenia przedstawiciel GIODO omówił najważniejsze skutki nowej regulacji dla polskiej praktyki funkcjonowania ochrony danych osobowych.

DEBATA Z OKAZJI ŚWIATOWEGO DNIA KONSUMENTA, WARSZAWA, 16.03.2016

O tym, jak obowiązujące przepisy konsumenckie są respektowane przez przedsiębiorców oraz o relacji pomiędzy ustawą o prawach konsumenta a prawem telekomunikacyjnym, dyskutowano podczas debaty pn. „Konsument na rynku usług telekomunikacyjnych oraz e-commerce" z okazji Światowego Dnia Konsumenta. Przedstawiciel GIODO wygłosił prezentację dotyczącą powiązania aktów prawnych regulujących obszar komunikacji marketingowej oraz prawidłowego uzyskiwania zgody na jej otrzymywanie. Organizatorem tego wydarzenia był Urząd Ochrony Konkurencji i Konsumentów.

KONFERENCJA NAUKOWA PT. „WPŁYW E-ZDROWIA NA JAKOŚĆ i KOSZTY OPIEKI ZDROWOTNEJ", WARSZAWA, 1.04.2016

Omówieniu korzyści i problemów płynących z wprowadzenia rozwiązań e-zdrowia, w szczególności z perspektywie doświadczeń innych krajów w tym zakresie, poświęcona była Konferencja zorganizowana na Warszawskim Uniwersytecie Medycznym przez Polskie Towarzystwo Ekonomiki Zdrowia. W spotkaniu tym uczestniczył przedstawiciel GIODO, który przedstawił prezentację poświęconą ochronie danych osobowych w elektronicznej dokumentacji medycznej.

KONFERENCJA PT. „BADANIA i INNOWACJE W OBSZARZE BEZPIECZEŃSTWA – WYMIANA MIĘDZYNARODOWYCH DOŚWIADCZEŃ", WARSZAWA, 12.05.2016

Identyfikacja i wypracowanie optymalnych sposobów współpracy pomiędzy przedstawicielami nauki, przedsiębiorcami oraz służbami

i instytucjami odpowiedzialnymi za bezpieczeństwo, w ramach prac badawczo-rozwojowych, były głównym tematem Konferencji zorganizowanej przez Polską Platformę Bezpieczeństwa Wewnętrznego wraz z Krajowym Punktem Kontaktowym Programów Badawczych Unii Europejskiej. Przedstawiciel GIODO uczestniczył w dyskusji na temat zachowania równowagi pomiędzy prawem do prywatności i ochrony danych osobowych a koniecznością inwigilacji.

KONFERENCJA PT. „INWIGILACJA, ILE MOŻNA?”, WARSZAWA, 14.05.2016

Zagadnienia dotyczące przetwarzania informacji i danych osobowych przez służby specjalne w ramach wykonywania zadań związanych z bezpieczeństwem Państwa i obywateli były głównym tematem Konferencji zorganizowanej przez Naczelną Radę Adwokacką i Komisję Praw Człowieka działającą przy NRA, w gmachu Biblioteki Uniwersyteckiej w Warszawie. Dyskutowano nad efektywnością kontroli sprawowanej nad służbami specjalnymi przez różne instytucje, w kontekście zachowania równowagi pomiędzy bezpieczeństwem a prawami człowieka i wolnościami obywatelskimi. Unijnym standardom przetwarzania danych osobowych przez organy ścigania na tle relacji transatlantyckich poświęcone było wystąpienie przedstawiciela Generalnego Inspektora Ochrony Danych Osobowych.

XX FORUM ADO/ABI, WARSZAWA, 17.05.2016

Tematyka tej jubileuszowej Konferencji koncentrowała się na przepisach nowego europejskiego prawa ochrony danych osobowych i jego wpływie na regulacje i praktykę obowiązującą w Polsce. Podczas tego Forum Zastępca GIODO, w wystąpieniu pt. „Kierunki zmian w systemie ochrony danych osobowych wobec wejścia w życie ogólnego rozporządzenia o ochronie danych osobowych”, przedstawił kluczowe instytucje prawa ochrony danych osobowych, które ulegną zmianie wraz z wejściem w życie ogólnego rozporządzenia, a także zwrócił uwagę na konieczność uregulowania tych zagadnień, które nie zostały objęte tym rozporządzeniem. Zasygnalizował też konieczność przeanalizowania brzmienia przepisów dotyczących prowadzenia postępowań przez GIODO, m.in. W związku z nałożeniem na organ ds. ochrony danych osobowych nowych obowiązków, a także biorąc pod uwagę możliwość zwiększenia szybkości i efektywności postępowania. Organizatorem XX Forum ADO/ABI było Centrum Promocji Informatyki.

KONFERENCJA „UDOSTĘPNIANIE WYNIKÓW BADAŃ KLINICZNYCH – PRZYWILEJ CZY OBOWIĄZEK? KRAKÓW, 20.05.2016

Kwestia otwartego dostępu do wyników badań klinicznych, w szczególności w kontekście ochrony danych osobowych pacjentów, była tematem przewodnim Konferencji zorganizowanej w Krakowie z okazji Międzynarodowego Dnia Badań Klinicznych. Podczas tego spotkania przedstawiciel GIODO wygłosił prezentację pt. „Warunki przetwarzania danych zawartych w dokumentacji badań klinicznych w świetle nowych ram ochrony danych osobowych w UE”. Organizatorzy: Uniwersytet Jagielloński – Collegium Medicum oraz Cochrane Polska.

SEMINARIUM PODSUMOWUJĄCE VI EDYCJĘ OGÓLNOPOLSKIEGO PROGRAMU EDUKACYJNEGO GIODO, WARSZAWA, 7.06.2016

Seminarium podsumowujące VI edycję Ogólnopolskiego Programu Edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli" odbyło się 7 czerwca 2016 r. W Pałacu Staszica w Warszawie. W uroczystym otwarciu seminarium wzięli udział partnerzy Programu - Minister Edukacji Narodowej i Rzecznik Praw Dziecka, a także przedstawiciel Ministerstwa Cyfryzacji. Podczas seminarium wręczono nagrody i wyróżnienia w konkursach zorganizowanych przez GIODO w ramach VI edycji Programu. Szkoły Nagrodzone w konkursie na najciekawszą inicjatywę edukacyjną miały również okazję przedstawić swoje przedsięwzięcia, zaś uczniowie biorący udział w konkursie fotograficznym – zaprezentować swoje prace.

KONFERENCJA „INSPEKTOR OCHRONY DANYCH – KONTYNUATOR ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI CZY NOWA FUNKCJA ZAPEWNIAJĄCA PRZESTRZEGANIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH?", WARSZAWA, 29.06.2016

W dniu 29 czerwca 2016 r. W Pałacu Staszica w Warszawie odbyła się konferencja kończąca i edycję studiów podyplomowych „Wykonywanie funkcji administratora bezpieczeństwa informacji", które pod patronatem Generalnego Inspektora Ochrony Danych Osobowych oraz Stowarzyszenia Administratorów Bezpieczeństwa Informacji uruchomione zostały w Instytucie Nauk Prawnych PAN w roku akademickim 2015/2016. Konferencja poświęcona została problematyce funkcji inspektora ochrony danych, który od 25 maja 2018 r. ma przejąć zadania wykonywane dotychczas przez administratora bezpieczeństwa informacji (ABI).

SEMINARIUM „NOWE PRZEPISY O OCHRONIE DANYCH OSOBOWYCH. WDROŻENIE OGÓLNEGO ROZPORZĄDZENIA UE O OCHRONIE DANYCH", WARSZAWA, 7.07.2016

Omówieniu przepisów ogólnego rozporządzenia o ochronie danych osobowych i przygotowaniu do ich stosowania w polskim systemie prawnym, poświęcone było seminarium zorganizowane przez Polskie Stowarzyszenie Prawników Przedsiębiorstw i kancelarię prawną PwC Legal we współpracy z GIODO. Podczas seminarium odbyło się także wręczenie nagród laureatom VI edycji konkursu dla studentów kierunku prawo i administracja, dotyczący wybranego zagadnienia ochrony danych osobowych organizowanego przez GIODO przy wsparciu merytorycznym kancelarii prawnej PwC Legal.

KONFERENCJA NT. ZMIAN W SYSTEMIE OCHRONY DANYCH OSOBOWYCH, LUBLIN, 14.09.2016

Omówieniu zmian, jakie w systemie ochrony danych osobowych wprowadzi ogólne rozporządzenie o ochronie danych osobowych, poświęcona była Konferencja zorganizowana przez Lubelską Izbę Rzemieślniczą. Przedstawione w niej zostały główne kierunki zmian prawa ochrony danych osobowych i ich praktyczne implikacje, a także rola administratora bezpieczeństwa informacji (ABI), przyszłego inspektora ochrony danych, i gwaranta właściwego przetwarzania danych osobowych.

XII KONFERENCJA „BIOMETRIA 2016”, WARSZAWA, 22.09.2016

Zagadnienia związane z definiowaniem danych biometrycznych w kontekście przetwarzania danych osobowych przy użyciu systemów informatycznych oraz ocena ich zgodności z przepisami prawa, były głównym tematem wystąpienia przedstawiciela GIODO podczas XII Konferencji „BIOMETRIA 2016”. Omówione zostały wytyczne Grupy Roboczej Art. 29 w tym zakresie oraz przytoczono przykłady sporów interpretacyjnych w zakresie legalności przetwarzania danych biometrycznych, zakończonych wyrokiem sądowym. Organizatorami tego wydarzenia była Politechnika Warszawska oraz Instytut Maszyn Matematycznych.

MIĘDZYNARODOWA KONFERENCJA „TRUSTED ID SUMMIT”, WARSZAWA, 22.09.2016

Aktualne wyzwania stojące przed ochroną danych osobowych w związku z możliwością automatycznej weryfikacji tożsamości klientów były tematem Międzynarodowej Konferencji „TRUSTED ID SUMMIT”, której organizatorem był Medien Service. W trakcie spotkania przedstawione zostały nowoczesne metody weryfikacji i identyfikacji klienta, z uwzględnieniem regulacji takich jak rozporządzenie eIDAS i dyrektywa PSD2 dotycząca identyfikacji i bezpieczeństwa usług płatniczych.

XXII FORUM TELEINFORMATYKI, MIEDZESZYN, 29-30.09.2016

Budowa nowoczesnego Państwa opartego na powszechnym wykorzystaniu technologii teleinformatycznych nie jest celem antagonistycznym dla nikogo – pod takich hasłem przebiegało XXII Forum Teleinformatyki, pt. „Państwo w cyberprzestrzeni”, które pod honorowym patronatem GIODO odbywało się w Miedzeszynie. Od kilku lat stałym punktem programu jest sesja Forum Młodych Mistrzów, której celem jest popularyzacja w środowisku młodych naukowców, ekonomicznych i prawnych zagadnień teleinformatyki w administracji publicznej. Generalny Inspektor jest patronem nagrody przyznawanej za najlepszą prezentację z zakresu ochrony danych osobowych wygłoszoną podczas tej sesji. Uroczystość wręczenia nagród Młodym Mistrzom Informatyki odbyła się 12 grudnia 2016 r. W Ministerstwie Cyfryzacji.

KONFERENCJA „FUNKCJONOWANIE BIG DATA PO WEJŚCIU W ŻYCIE ROZPORZĄDZENIA OGÓLNEGO W ZAKRESIE OCHRONY DANYCH OSOBOWYCH”, WARSZAWA, 4.10.2016

Celem Konferencji było zwrócenie uwagi przedstawicieli polskiego sektora bankowego na problematykę ochrony danych osobowych w ramach świadczenia usług bankowych, w kontekście wykorzystania technologii BIG DATA oraz zmian prawnych wprowadzanych rozporządzeniem ogólnym o ochronie danych osobowych. Wystąpienie przedstawiciela GIODO dotyczyło zagadnień bezpieczeństwa danych osobowych zgromadzonych w bazach danych, szansom i wyzwaniom dla sektora finansowego w związku z profilowaniem danych klientów oraz poszukiwaniu źródeł dodatkowych danych. Organizatorem tego wydarzenia był Związek Banków Polskich.

KONFERENCJA „NOWE REGULACJE W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W SEKTORZE FINANSOWYM”, WARSZAWA, 11.10.2016

Problematyka przetwarzania danych osobowych klienta w kontekście nowych regulacji o ochronie danych osobowych, były głównym tematem obrad konferencji, podczas których przedstawiciel GIODO omówił zagadnienia związane z zakresem swobody we wdrażaniu nowych przepisów oraz odpowiedzialności podmiotów za niewdrożenie lub niepełne wdrożenie nowych regulacji. Ważnym tematem było także przeciwdziałanie nadużyciom oraz przestępstwom w świetle nowego rozporządzenia ogólnego o ochronie danych osobowych.

V KONWENT OCHRONY DANYCH OSOBOWYCH I INFORMACJI, ŁÓDŹ, 15.11.2016

O tym, jak zabezpieczyć dane osobowe i ocenić ryzyko naruszenia, kwestie wdrożenia odpowiednich środków bezpieczeństwa w celu zapewnienia poufności i integralności przetwarzanych danych, a także możliwości wykorzystania pseudonomizacji jako środka zabezpieczającego dane oraz anonimizacji jako narzędzia do dalszego ich wykorzystania po wygaśnięciu pierwotnego celu ich przetwarzania, były głównym tematem V Konwentu. Przedstawiciel GIODO przedstawił prezentację dotyczącą koniecznych działań przygotowujących do pełnienia funkcji Administratora Bezpieczeństwa Informacji – w przyszłości Inspektora Ochrony Danych – w świetle nowego rozporządzenia unijnego o ochronie danych osobowych (RODO). V edycja Konwentu zorganizowana była przy współpracy ForSafe Sp. Z o.o. oraz Lubasz i Wspólnicy Kancelarii Radców Prawnych.

KONFERENCJA „PRAWA DZIECKA w KONSTELACJI RODZINNEJ I PLACÓWEK OŚWIATOWYCH”, WARSZAWA, 15.11.2016

Generalny Inspektor Ochrony Danych Osobowych, Rzecznik Praw Dziecka oraz Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, byli inicjatorami cyklu ogólnopolskich konferencji naukowych poświęconych prawom dziecka w obszarach społecznych. Tematyka pierwszej z nich, zorganizowanej 15 listopada 2016 r. na UKSW, odnosiła się do kwestii poszanowania praw dziecka w rodzinie oraz w codziennej działalności placówek oświatowych.

KONFERENCJA „KRADZIEŻ TOŻSAMOŚCI W INTERNECIE”, WARSZAWA, 22.11.2016

Wykorzystywanie cudzych danych osobowych bez wiedzy i zgody osoby, której dane dotyczą oraz zapobieganie temu coraz bardziej powszechnemu zjawisku, poświęcona była Konferencja, której organizatorami byli Generalny Inspektor Ochrony Danych Osobowych, Ministerstwo Spraw Wewnętrznych i Administracji oraz Wydział Administracji i Nauk Społecznych Politechniki Warszawskiej. Zagrożenie bezpieczeństwa danych osobowych może dotyczyć niemal wszystkich aspektów życia prywatnego i zawodowego, stając się pierwszym krokiem na drodze do popełnienia kolejnych czynów zabronionych. i dlatego uczestnicy tego spotkania zgodni byli co do potrzeby kontynuowania działań w ramach szeroko rozumianej edukacji społecznej, wskazując jednocześnie na potrzebę poszerzenia zakresu ochrony prawno-karnej, w celu wzmocnienia ochrony praw jednostki – podmiotu danych.

XI FORUM KIEROWNIKÓW JEDNOSTEK ORGANIZACYJNYCH ORAZ PEŁNOMOCNIKÓW DS. OCHRONY INFORMACJI NIEJAWNYCH, ZAKOPANE, 23-25.11.2016

Spotkanie to poświęcone było zagadnieniom związanym z funkcjonowaniem pionów ochrony w firmach i w instytucjach, w kontekście występujących wyzwań i zagrożeń bezpieczeństwa informacji, w tym danych osobowych. Przedstawiona została ewaluacja roli i zadań pionów ochrony informacji niejawnych na przestrzeni kilku lat. Podczas tego wydarzenia, Zastępca Generalnego Inspektora Ochrony Danych Osobowych, wygłosił referat poświęcony aktualnej roli i rosnącemu znaczeniu ADO i ABI oraz współdziałaniu Kierowników Jednostek Organizacyjnych i Pełnomocników ds. Ochrony Informacji Niejawnych w nowych relacjach prawnych. Organizatorem XI Forum było Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.

KONFERENCJA „DRONY JAKO ŹRÓDŁO NOWYCH MIEJSC PRACY I WZROSTU GOSPODARCZEGO”, WARSZAWA, 24.11.2016

Drony posiadające możliwość nagrywania obrazu i dźwięku mogą – poprzez niewłaściwe ich użytkowanie – stanowić zagrożenie dla prywatności. Naruszenie przestrzeni prywatnej przez drony bez zgody osób nagrywanych, czy brak świadomości użytkowników dronów o obowiązku związanych z ochroną danych osobowych są jednym z największych problemów związanych z szybko rozwijającym się w Polsce rynkiem dronów. Podczas Konferencji przedstawiciel GIODO wygłosił na ten temat referat wskazując na konieczność odpowiedzialnego korzystania z tej nowoczesnej technologii. na zakończenie tego spotkania przyjęta została Deklaracja Warszawska zawierająca listę konkretnych działań w celu urzeczywistnienia wspólnego, jednolitego rynku dronów w Unii Europejskiej. Organizatorami Konferencji byli: Ministerstwo Infrastruktury i Budownictwa, Urząd Lotnictwa Cywilnego oraz Europejska Agencja Bezpieczeństwa Lotniczego (EASA).

KONFERENCJA „WDROŻENIE OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH – ASPEKTY PROCEDURALNE”, WARSZAWA, 7.12.2016

Podczas Konferencji omówione zostały najważniejsze kwestie związane z problematyką szeroko rozumianych aspektów proceduralnych związanych z wdrożeniem ogólnego rozporządzenia o ochronie danych, takie jak poszanowanie autonomii proceduralnej państw członkowskich w procesie wdrożenia przepisów rozporządzenia, zasady postępowania przed Generalnym Inspektorem Ochrony Danych Osobowych w kontekście efektywności i gwarancji proceduralnych, jak również rola sądów w postępowaniach z zakresu ochrony danych osobowych. Konferencja była też okazją do przedyskutowania nowych koncepcji, jak zastosowanie mediacji do rozstrzygania spraw z zakresu ochrony danych osobowych czy możliwe rozwiązania mające na celu zapewnienie sądowej kontroli stosowania administracyjnych kar pieniężnych przez organ nadzorczy. Organizatorami Konferencji byli Generalny Inspektor Ochrony Danych Osobowych, Prezes Naczelnego Sądu Administracyjnego oraz Dziekan Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.

1.6. Porozumienia o współpracy

POLSKA IZBA INFORMATYKI I TELEKOMUNIKACJI, WARSZAWA, 16.10.2016

Uroczystość podpisania porozumienia o współpracy miała miejsce 16 grudnia 2016 r. W Warszawie, podczas Konferencji pt. „Ochrona danych osobowych – wyzwania dla sektora teleinformatycznego w perspektywie rozporządzenia o ochronie danych osobowych", której organizatorami byli GIODO i PIIiT.

Współpraca obu podmiotów ma się przyczynić do doskonalenia jakości i standardów ochrony danych osobowych w sektorze teleinformatycznym, zwłaszcza zaś do przygotowania działających w tym obszarze podmiotów do właściwego stosowania nowych zasad ochrony danych osobowych, które wprowadza rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwane ogólnym rozporządzeniem o ochronie danych).

Porozumienie zawarte między Generalnym Inspektorem Ochrony Danych Osobowych (GIODO) a Polską Izbą Informatyki i Telekomunikacji (PIIiT) przewiduje ponadto, że Izba stworzy kodeks postępowania, który zostanie opracowany zgodnie z wymaganiami powyższego rozporządzenia, a także przepisami prawa krajowego oraz z uwzględnieniem specyfiki sektora teleinformatycznego. GIODO będzie zaś udzielał niezbędnych informacji pomocnych w opracowaniu takiego dokumentu.

RZECZNIK PRAW DZIECKA, WARSZAWA, 12.10.2016

Porozumienie pomiędzy Rzecznikiem Praw Dziecka Markiem Michalakiem a Generalnym Inspektorem Ochrony Danych Osobowych dr Edytą Bielak-Jomaa, określa zasady współpracy w realizacji ustawowych zadań dla podniesienia skuteczności poprawy stanu przestrzegania zasad ochrony danych osobowych oraz rozwiązywania problemów stanowiących przedmiot wspólnego zainteresowania Stron.

Współpraca obejmuje wzajemną wymianę wiedzy i doświadczeń wynikających z działań realizowanych przez każdą ze Stron w ramach swoich kompetencji, w zakresie spraw objętych współdziałaniem, a także działania mające na celu podnoszenie kwalifikacji pracowników Biura RPD i Biura GIODO, w tym współpracę przy opracowywaniu programów szkoleń, wymianę wykładowców, zapewnienie pracownikom – w miarę zgłaszanych potrzeb i możliwości – udziału w kursach, szkoleniach i innych działaniach organizowanych przez Strony, prowadzenie wspólnych działań w uzgodnionym zakresie tematycznym, w tym wspólnych działań o charakterze edukacyjnym, wzajemne przekazywanie informacji i sygnałów o występujących nieprawidłowościach, które mogą stanowić przedmiot zainteresowania Stron.

UNIWERSYTET MARII CURIE-SKŁODOWSKIEJ W LUBLINIE, LUBLIN, 14.09.2016

GIODO i Uniwersytet Marii Curie-Skłodowskiej w Lublinie zawarli porozumienie o współpracy, a jego uroczyste podpisanie odbyło się

14 września 2016 r. W siedzibie uczelni. W imieniu UMCS porozumienie podpisał JM Rektor UMCS prof. dr hab. Stanisław Michałowski, a ze strony GIODO – dr Edyta Bielak-Jomaa, Generalny Inspektor Ochrony Danych Osobowych.

Podczas uroczystości obecni byli także: prof. Andrzej Kidyba, kierownik Katedry Prawa Gospodarczego i Handlowego na Wydziale Prawa i Administracji UMCS oraz Andrzej Lewiński, zastępca Generalnego Inspektora Ochrony Danych Osobowych.

Porozumienie przewiduje, że GIODO i UMCS będą prowadzić wspólne przedsięwzięcia o charakterze naukowo-badawczym, edukacyjnym, promocyjnym i wydawniczym. W planach jest organizacja seminariów, wykładów, konferencji i szkoleń, a także praktyk studenckich oraz studiów podyplomowych. Strony zadeklarowały, że będą też wspólnie inicjować prace naukowe i badawcze z zakresu ochrony danych osobowych.

KRAJOWA SPÓŁDZIELCZA KASA OSZCZĘDNOŚCIOWO-KREDYTOWA, SOPOT, 7.09.2016

Wspólne działanie na rzecz podnoszenia poziomu ochrony danych osobowych w działalności spółdzielczych kas oszczędnościowo-kredytowych oraz stworzenie kodeksu postępowania to główne założenia tego dokumentu.

Porozumienie przewiduje, że podejmowane przez SKOK działania uwzględniać będą europejskie i polskie regulacje prawne z zakresu ochrony danych osobowych. Szczególny nacisk położony zostanie na konieczność efektywnego dostosowania się do nowych zasad ochrony danych osobowych, które wprowadza rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Będą one uwzględnione także w treści kodeksu postępowania w zakresie ochrony danych osobowych, który ma zostać opracowany przez SKOK. GIODO zobowiązał się zaś do udzielania niezbędnych informacji pomocnych w opracowaniu takiego dokumentu.

Porozumienie zostało podpisane 7 września 2016 r. W Sopocie. Parafowali je: minister Andrzej Lewiński, zastępca Generalnego Inspektora Ochrony Danych Osobowych (GIODO) oraz Rafał Matusiak, prezes Zarządu Krajowej Kasy oraz Wiktor Kamiński, pełnomocnik Krajowej Kasy.

SKOK-i to kolejny, po Związku Banków Polskich, podmiot z sektora bankowego, który do przetwarzania danych osobowych postanowił podejść ze szczególną troską i w sposób kompleksowy.

UNIWERSYTET GDAŃSKI, GDAŃSK, 24.05.2016

Stroną porozumienia o współpracy GIODO z Uniwersytetem Gdańskim był Prof. dr hab. Jakub Stelina, Dziekan Wydziału Prawa i Administracji.

Współpraca obejmuje wspólne przedsięwzięcia w obszarze działalności naukowo-badawczej, edukacyjnej, promocyjnej, wydawniczej, a także organizacyjnej, związanej z m.in. planowanym uruchomieniem na tych Uczelniach studiów podyplomowych dotyczących zagadnień związanych z ochroną prywatności i bezpieczeństwa danych osobowych.

AKADEMIA MARYNARKI WOJENNEJ IM. BOHATERÓW WESTERPLATTE W GDYNI, GDYNIA, 23.05.2016

Uroczystość podpisania porozumienia o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych reprezentowanym przez Pana Ministra Andrzeja Lewińskiego, Zastępcę GIODO, a Akademią Marynarki Wojennej im. Bohaterów Westerplatte, reprezentowaną przez Rektora-Komendanta kmdr prof. dr hab. Tomasza Szubrychta, odbyła się w siedzibie tej uczelni w dniu 23 maja 2016 r.

Współpraca obejmuje wspólne przedsięwzięcia w obszarze działalności naukowo-badawczej, edukacyjnej, promocyjnej, wydawniczej, a także organizacyjnej, związanej z m.in. planowanym uruchomieniem na tych Uczelniach studiów podyplomowych dotyczących zagadnień związanych z ochroną prywatności i bezpieczeństwa danych osobowych.

POLSKA IZBA UBEZPIECZEŃ, SOPOT, 10.05.2016

Wspólne działanie na rzecz podnoszenia poziomu ochrony danych osobowych – to główne założenia porozumienia zawartego między Generalnym Inspektorem Ochrony Danych Osobowych a Polską Izbą Ubezpieczeń. Porozumienie przewiduje, że strony będą współpracować na rzecz podnoszenia poziomu ochrony danych osobowych oraz w celu właściwego stosowania przez członków Polskiej Izby Ubezpieczeń przepisów rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych opublikowanego 4 maja 2016 r., które zacznie obowiązywać we wszystkich krajach unijnych 25 maja 2018 r. PIU zobowiązało się, że podejmie działania w celu stworzenia kodeksu postępowania w zakresie ochrony danych osobowych w działalności ubezpieczeniowej i reasekuracyjnej. Kodeks przygotowany będzie zgodnie z wymaganiami ogólnego rozporządzenia o ochronie danych, przepisami prawa krajowego oraz z uwzględnieniem specyfiki sektora ubezpieczeniowego. GIODO zobowiązał się zaś do udzielania niezbędnych informacji pomocnych w opracowaniu takiego dokumentu.

Minister Andrzej Lewiński, zastępca Generalnego Inspektora Ochrony Danych Osobowych i J. Grzegorz Prądzyński, prezes zarządu Polskiej Izby Ubezpieczeń (PIU) podpisali porozumienie 10 maja 2016 r. W Sopocie podczas IV Kongresu PIU.

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU, TORUŃ, 15.03.2016

W dniu 15 marca 2016 r., podczas posiedzenia Rady Wydziału Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, podpisane zostało porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych reprezentowanym przez Pana Ministra Andrzeja Lewińskiego, Zastępcę GIODO a Wydziałem Prawa i Administracji UMK w Toruniu, reprezentowanym przez Pana Dziekana dr hab. Arkadiusza Lacha, prof. UMK. Współpraca obejmuje wspólne przedsięwzięcia w obszarze działalności naukowo-badawczej, edukacyjnej, promocyjnej, wydawniczej, a także organizacyjnej, związanej z m.in. planowanym uruchomieniem na tej Uczelni studiów podyplomowych dotyczących zagadnień związanych z ochroną danych osobowych.

Porozumienie jest efektem dotychczasowej wieloletniej współpracy Uniwersytetu Mikołaja

Kopernika w Toruniu i Generalnego Inspektora Ochrony Danych Osobowych w zakresie właściwego stosowania przepisów ustawy o ochronie danych osobowych, w szczególności w obszarze bezpieczeństwa sieci i informacji, a także współorganizacji spotkań i konferencji na ten temat.

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO, WARSZAWA, 23.02.2016

W dniu 23 maja 2016 r. podpisane zostało nowe porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy dr Edytą Bielak-Jomaa, Generalnym Inspektorem Ochrony Danych Osobowych a JM Rektorem ks. prof. dr hab. Stanisławem Dziekońskim, w ramach którego Strony zobowiązały się świadczyć wzajemną pomoc w ramach swoich kompetencji określonych w odpowiednich przepisach.

Dążąc do podwyższenia poziomu wiedzy zawodowej i profesjonalnych umiejętności praktycznych oraz doskonalenia mechanizmów działalności w zakresie ochrony prywatności i danych osobowych, Strony będą organizować seminaria, wykłady, konferencje, szkolenia, praktyki studenckie, studia podyplomowe oraz inicjować prace naukowe i badawcze z zakresu ochrony danych osobowych.

W celu zapewnienia, by wiedza przekazywana w toku procesu kształcenia była na najwyższym poziomie i zgodna ze stanowiskami GIODO w sprawach, które były przedmiotem jego rozstrzygnięć, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie będzie przekazywał informacje na temat planowanych przedsięwzięć związanych z problematyką prawa do prywatności i ochrony danych osobowych, a także zapewni możliwość wglądu i konsultacji treści programów nauczanych przedmiotów z tego zakresu, w szczególności w ramach podyplomowych studiów.

WYŻSZA SZKOŁA BIZNESU W DĄBROWIE GÓRNICZEJ, 14.01.2016

W dniu 14 stycznia 2016 r. podpisany został Aneks do Porozumienia zawartego 5 października 2011 r. pomiędzy Generalnym Inspektorem Ochrony Danych osobowych dr Wojciechem R. Wiewiórowskim a Jej Magnificencją Rektor Wyższej Szkoły Biznesu w Dąbrowie Górniczej prof. nadzw. dr Zdzisławą Dacko-Pikiewicz, o współpracy w zakresie ochrony prywatności i danych osobowych.

Aneks dotyczy zapisu w kwestii przekazywania GIODO informacji na temat planowanych przedsięwzięć związanych z ochroną danych osobowych i prawem do prywatności, a także zapewnienia wglądu i możliwości konsultacji treści programów nauczanych przedmiotów z tego zakresu, w szczególności w ramach podyplomowych studiów.

UNIWERSYTET ŚLĄSKI W KATOWICACH, KATOWICE, 13.01.2016

Nowe porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy Generalnym Inspektorem Ochrony Danych Osobowych dr Edytą Bielak-Jomaa a Uniwersytetem Śląskim w Katowicach, reprezentowanym przez JM Rektora prof. Zw. dr hab. Wiesława Banysia, określa zasady wzajemnej pomocy przy realizacji Porozumienia.

Dążąc do podwyższenia poziomu wiedzy zawodowej i profesjonalnych umiejętności praktycznych oraz doskonalenia mechanizmów działalności w zakresie ochrony prywatności i danych osobowych, Strony będą organizo-

wać seminaria, wykłady, konferencje, szkolenia, praktyki studenckie, studia podyplomowe oraz inicjować prace naukowe i badawcze z zakresu ochrony danych osobowych.

W celu zapewnienia, by wiedza przekazywana w toku procesu kształcenia była na najwyższym poziomie i zgodna ze stanowiskami GIODO w sprawach, które były przedmiotem jego rozstrzygnięć, Uniwersytet Śląski w Katowicach będzie przekazywał informacje na temat planowanych przedsięwzięć związanych z problematyką prawa do prywatności i ochrony danych osobowych, a także zapewni możliwość wglądu i konsultacji treści programów nauczanych przedmiotów z tego zakresu, w szczególności w ramach podyplomowych studiów.

Pierwsze porozumienie o współpracy pomiędzy GIODO a Uniwersytetem Śląskim w Katowicach podpisane było 23 października 2010 roku.

2. Działalność informacyjna

W 2016 r. stronę internetową www.giodo.gov.pl odwiedzono – ponad 5 mln razy.

Z inicjatywy GIODO w mediach ukazało się ponad 150 materiałów prasowych o tematyce ochrony danych. Dziennikarzom kontaktującym się z urzędem udzielono ponad 300 odpowiedzi na pytania. GIODO lub eksperci z Biura udzielili ponad 70 wywiadów.

W 2016 r. działalność informacyjna GIODO prowadzona była, podobnie jak w latach ubiegłych, za pośrednictwem różnorodnych kanałów komunikacyjnych, takich jak:

- strona internetowa GIODO (na bieżąco aktualizowana i uzupełniana),
- media tradycyjne i elektroniczne,
- konferencje i seminaria naukowe (organizowane zarówno przez GIODO, jak i inne instytucje współpracujące z GIODO),
- 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 z-cę GIODO i pracowników departamentów,
- publikacje książkowe.

STRONA INTERNETOWA

Stale aktualizowana strona internetowa to jeden z podstawowych kanałów informowania o bieżącej pracy urzędu – wydanych decyzjach, interpretacjach prawnych, wynikach prowadzonych przez GIODO kontroli, opiniach na temat projektów aktów prawnych, ważnych spotkaniach i porozumieniach.

Strona ta cieszy się bardzo dużą oglądalnością – w roku 2016 odwiedzono ją ponad 5 mln razy. Ponad połowa tych wizyt to wejścia stałych użytkowników portalu.

Ważną funkcją strony internetowej GIODO jest dostarczanie fachowych porad różnym grupom odbiorców, zarówno administratorom danych, jak i osobom, których dane dotyczą. W 2016 r. GIODO, biorąc pod uwagę rosnącą

rolę i znaczenie administratorów bezpieczeństwa informacji (ABI) – przyszłych inspektorów ochrony danych, którzy będąc fachowym wsparciem dla administratorów danych, są jednocześnie filarem, na którym oprzeć można system skutecznej ochrony danych osobowych danej instytucji, uruchomił na swojej stronie internetowej **nowy serwis**, skierowany do tej grupy osób – **„ABI Informator"**. Znalazły się w nim m.in. informacje dotyczące statusu i zadań ABI, wskazówki co do powoływania takich osób w firmach i ich zgłaszania do rejestru GIODO, a także materiały dotyczące prowadzenia przez ABI sprawdzeń na zlecenie GIODO. Jedną z części stale rozbudowywanego serwisu są też odpowiedzi na najczęściej zadawane pytania.

STAŁA WSPÓŁPRACA ZE ŚRODKAMI MASOWEGO PRZEKAZU

Wzorem lat ubiegłych, w 2016 r. GIODO, realizując cele informacyjno-edukacyjne, kontynuował stałą współpracę z mediami polegającą m.in. 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. „IT w Administracji", „Gazetą Ubezpieczeniową") oraz portalami internetowymi (jak np. Dziennik Internautów czy lex.pl), w tym będącymi odpowiednikami prasy drukowanej. Upowszechnianiu wiedzy z zakresu ochrony danych osobowych służyła też publikacja wyjaśnień GIODO w czasopismach kobiecych, takich jak np. „Twoje Imperium", „Tina" czy „Świat Kobiety". W 2016 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 dla Ciebie, TVP INFO, Telewizją Polsat. Zaowocowała ona emisją wielu programów o tematyce ochrony danych osobowych.

Przekazywane przez GIODO materiały i informacje dotyczące tej problematyki chętnie wykorzystywały również współpracujące z GIODO agencje informacyjne, zwłaszcza PAP.

W 2016 r. W prasie, radiu, telewizji i Internecie opublikowanych lub wyemitowanych zostało – zainicjowanych przez GIODO – **ponad 150 materiałów prasowych o tematyce ochrony danych**. Przeważająca ich część jest dostępna na stronie internetowej GIODO www.giodo.gov.pl.

W 2016 r. GIODO nawiązał też stałą współpracę z nowym pismem branżowym – kwartalnikiem „ABI Expert", w którym uruchomił stałą rubrykę informacyjną.

ODPOWIEDZI NA INDYWIDUALNE PYTANIA DZIENNIKARZY

Stałą formą kontaktów GIODO z dziennikarzami było udzielanie im odpowiedzi na pytania, które dotyczyły ochrony danych osobowych w wielu różnorodnych sytuacjach.

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,
- wykorzystywanie danych osobowych na potrzeby marketingu, ze szczególnym uwzględnieniem jednej z jego form, tj. telemarketingu,
- udostępnianie nieznanym podmiotom - przez osoby, których dane dotyczą - szczegółowych informacji na swój temat; sposoby wyłudzania danych i zagrożenia z tym związane,
- 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,
- 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,
- możliwość stosowania monitoringu wizyjnego przez instytucje inne, niż ustawowo upoważnione,
- pozyskiwanie danych osobowych przez wspólnoty i spółdzielnie mieszkaniowe,
- przetwarzanie danych osobowych w związku z rejestracją kart pre-paid,
- kwestia zakresu danych, które mogą być pozyskiwane w związku z głosowaniem na projekty finansowane ze środków budżetu obywatelskiego

WYWIADY GIODO I JEGO EKSPERTÓW

Tematyka wywiadów udzielanych prasie drukowanej i internetowej oraz radiu i telewizji 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 kwestia 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 billingów czy instalowanie monitoringu wizyjnego.

Częstym tematem rozmów było funkcjonowanie administratorów bezpieczeństwa informacji (ABI) – przyszłych inspektorów ochrony danych, zarówno w świetle obowiązujących przepisów, jak i po rozpoczęciu stosowania ogólnego rozporządzenia o ochronie danych.

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 w 2016 r. dotyczyło przetwarzania danych osobowych w sektorze oświaty i służby zdrowia, a także kwestii poszanowania prywatności w kontekście udostępniania informacji publicznej.

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 z nowoczesnych rozwiązań technologicznych w sektorze bankowym, a także dopuszczalności tworzenia przez przedsiębiorców profili osobowych klientów.

W 2016 r. GIODO oraz specjaliści z urzędu udzielili **ponad 70 wywiadów**.

AKCJE INFORMACYJNO-EDUKACYJNE

W 2016 r. obchody **Dnia Ochrony Danych Osobowych** (ustanowionego na 28 stycznia) odbywały się już po raz dziesiąty.

Z tej okazji, jak co roku, GIODO zorganizował konferencje poświęcone najaktualniejszym zagadnieniom dotyczącym prawa do prywatności i ochrony danych osobowych, jednak w 2016 r. Wydarzenia odbywające się z tej okazji miały wyjątkowy charakter i formułę. GIODO zaprosił bowiem do współorganizacji obchodów wyższe uczelnie, z którymi ma zawarte porozumienia o współpracy. W poszczególnych ośrodkach akademickich odbyły się więc konferencje poświęcone aktualnym problemom ochrony prywatności i danych osobowych, takim jak: Big Data (28 stycznia 2016 r., Warszawa), ochrona danych osobowych w służbie zdrowia (13 stycznia 2016 r., Katowice), ochrona danych w działalności marketingowej (14 stycznia 2016 r., Dąbrowa Górnicza), kradzież tożsamości (19 stycznia 2016 r., Szczytno) czy nowa rola i pozycja ABI (23 lutego 2016 r., Warszawa).

W wydarzeniach organizowanych przez GIODO i współpracujące z nim uczelnie wzięło udział **ponad 1500 osób z całego kraju**.

Jednocześnie poszczególnym konferencjom, towarzyszyły spotkania z mediami, które były okazją do poruszenia zarówno tematyki omawianej na konferencji, jak i innych zagadnień dotyczących ochrony danych osobowych i prywatności.

Tradycyjnie z okazji Dnia Ochrony Danych Osobowych GIODO oraz redakcja „Dziennika Gazety Prawnej zorganizowały wspólnie (11 stycznia 2016 r., w siedzibie Redakcji) debatę redakcyjną. Tym razem jej temat brzmiał „Big Data – korzyści i zagrożenia" Zapis z tej dyskusji opublikowany został na łamach Gazety 28 stycznia 2016 r.

Ponadto z okazji Dnia Ochrony Danych Osobowych okolicznościowy wywiad z GIODO na temat potrzeby i wagi ochrony danych osobowych ukazał się we wszystkich dziennikach regionalnych należących do Wydawnictwa Polska Press Grupa.

Co ważne, wszystkie tematy poruszane w czasie obchodów znalazły szeroki oddźwięk medialny, co z pewnością przekłada się na lepszą edukację zarówno osób, których dane dotyczą, i tych, którzy dane przetwarzają.

W 2016 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 informował w nim m.in., jak z danymi osobowymi klientów powinny postępować biura podróży i hotele – jakie dane mają prawo pozyskiwać i w jakich celach oraz jak długo wykorzystywać.

Ostrzegał też przed grożącymi nam negatywnymi konsekwencjami pozostawiania dowodu osobistego czy innych dokumentów potwierdzających tożsamość w zastaw za wypożyczony sprzęt. Przypominał jednocześnie, że to niedopuszczalna praktyka. Przetrzymywanie cudzego dowodu osobistego stanowi bowiem wykroczenie, za które zgodnie z ustawą o dowodach osobistych, grozi kara ograniczenia wolności do 1 miesiąca albo kara grzywny.

Ponadto GIODO radził, by przy zamieszczaniu w Internecie informacji związanych z wakacjami, w tym zdjęć, zachować rozwagę, by nie narazić się na różnego rodzaju nieprzyjemności.

Przestrzegał też, by z rozwagą udostępniać dane osobowe, odpowiadając na oferty sezonowego zatrudnienia, gdyż niektóre z nich są zamieszczane przez oszustów, próbujących jedynie wyłudzić dane osobowe osób ubiegających się o pracę, a nie je zatrudnić.

Radził też, jak się zachować, gdy utracimy dokument potwierdzający naszą tożsamość.

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.

IV. WSPÓŁPRACA MIĘDZYNARODOWA

1. 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.

Podkreślenia wymaga, że ww. Wiosenne Konferencje są najważniejszym, corocznym spotkaniem wszystkich rzeczników ochrony danych osobowych z państw członkowskich UE, innych państw europejskich oraz przedstawicieli Komisji Europejskiej, Rady Europy oraz innych organów zajmujących się ochroną danych osobowych. Poszczególne konferencje poświęcone są różnym aspektom ochrony danych osobowych w Europie, a ich uczestnicy podejmują działania ukierunkowane nie tylko na wdrażanie unijnych przepisów, ale

również na monitorowanie ich przestrzegania w poszczególnych krajach.

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).

W ramach współpracy na forum międzynarodowym, Generalny Inspektor Ochrony Danych Osobowych i jego przedstawiciele uczestniczyli w pracach różnych organów ochrony danych osobowych państw UE.

GRUPA ROBOCZA ART. 29

W omawianym roku sprawozdawczym 2016, 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 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.

W analizowanym roku 2016 Grupa Robocza Art. 29 skupiła się przede wszystkim na opracowaniu szeregu dokumentów dotyczących interpretacji i wdrażania rozporządzenia ogólnego o ochronie danych osobowych, w szczególności były to:

- Wytyczne i najczęściej zadawane pytania dotyczące **prawa do przenoszenia danych**,
- Wytyczne i najczęściej zadawane pytania dotyczące **inspektorów ochrony danych**,
- Wytyczne i najczęściej zadawane pytania dotyczące **wiodącego organu nadzorczego**.

Dodatkowo Grupa Robocza Art. 29 opracowała opinie dotyczące nowego porozumienia pomiędzy Unią Europejską a USA w sprawie przekazywania danych (Tarcza Prywatności), przeglądu dyrektywy o e-prywatności. Przygotowała także listy dotyczące wycieku danych z Yahoo, połączenia What's up z Facebookiem oraz list w sprawie zmian dotyczących

wielkoskalowych systemów IT Unii Europejskiej wykorzystywanych dla celów związanych z zarządzaniem granicami, polityką wizową i azylową, którego współsprawozdawcą był przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych.

GRUPA KOORDYNUJĄCA NADZÓR NAD SYSTEMEM INFORMACJI SCHENGEN DRUGIEJ GENERACJI – SIS II (SIS II SUPERVISION COORDINATION GROUP)

W 2016 roku Grupa SIS II pracowała m.in. nad metodologią prowadzenia czynności kontrolnych i wpisów w SIS II. Z inicjatywy polskiego organu ds. ochrony danych osobowych podjęła zadania związane kwestią dostępu do wpisów w SIS II w celach administracyjnych.

GRUPA KOORDYNUJĄCA NADZÓR NAD WIZOWYM SYSTEMEM INFORMACYJNYM – VIS (VIS SUPERVISION COORDINATION GROUP)

W 2016 roku Grupa VIS pracowała nad dokumentami dotyczącymi dostępu do danych przetwarzanych w VIS przez uprawnione organy oraz realizacji praw osób, których dane są przetwarzane w systemie. Ponadto sygnalizowała konieczność przeprowadzania audytów przez organy ochrony danych osobowych i zwracała uwagę na kwestie związane z przetwarzaniem danych osobowych przez dostawców zewnętrznych, którzy są odpowiedzialni za organizację pracy centrów wizowych.

GRUPA KOORDYNUJĄCA NADZÓR NAD SYSTEMEM EURODAC (EURODAC SUPERVISION COORDINATION GROUP)

Działalność tej Grupy skupiała się przede wszystkim na opracowaniu uwag do nowego rozporządzenia Eurodac. W rezultacie tych prac przygotowany został list zawierający uwagi i proponowane przepisy nowego rozporządzenia, którego adresatem była Rada Unii Europejskiej, Komisja Europejska i Parlament Europejski. Sprawozdawcą listu był przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych.

WSPÓLNY ORGAN NADZORCZY EUROPOLU (JOINT SUPERVISORY BODY OF EUROPOL)

W analizowanym roku sprawozdawczym 2016, organ ten skupił się przede wszystkim na opracowaniu regulaminu prac Rady Współpracy, która przejmie część funkcji Wspólnego Organu Nadzorczego Europolu (WON Europolu) w maju 2017 r. po rozpoczęciu stosowania nowego rozporządzenia o Europolu. Przedstawiciel GIODO był członkiem grupy, która opracowała przedmiotowy regulamin. Ponadto WON Europolu opracował także podręcznik o zasadach przekazywania danych do Jednostek Krajowych Europolu.

W tym miejscu podkreślenia wymaga, że w poprzednim roku sprawozdawczym, 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 pomię-

dzy 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.

Podsumowując, przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych pełni funkcję przewodniczącego **Wspólnego Organu Nadzorczego ds. Celnych (Joint Supervisory Authority Customs) oraz Grupy koordynującej nadzór nad Systemem Informacji Celnej – CIS (CIS Supervision Coordination Group).**

INNE

W ramach współpracy na forum międzynarodowym, przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych w 2016 r. uczestniczył w projekcie badawczym pod nazwą „Wymiana danych DNA w Unii Europejskiej: kontrola społeczna, obywatelska i demokratyczna" (Exchange of DNA data in the UE: Engaging Science with Social Control, Citizenship and Democracy). Celem tego badania była ocena wpływu wymiany danych DNA w UE na podstawie decyzji Pruem w wybranych państwach członkowskich. Projekt ten finansowany jest przez Europejską Radę Badań Naukowych.

2. 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.

KONFERENCJA O DRONACH, BUDAPESZT 5-6.02.2016

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).

MIĘDZYNARODOWA KONFERENCJA PROJEKTU ARCADES, BARCELONA, 4.03.2016

O potrzebie i sposobach edukowania dzieci i młodzieży z zakresu ochrony danych osobowych i prawa do prywatności dyskutowano na międzynarodowej konferencji zorganizowanej 4 marca 2016 roku w Barcelonie. Zorganizowanie tego wydarzenia było możliwe dzięki projektowi ARCADES realizowanemu przez GIODO ze środków Unii Europejskiej. W konferencji uczestniczyli przedstawiciele szkół i instytucji edukacyjnych oraz organizacji społecznych, przedstawiciele organów ochrony danych z m.in. Z Polski, Węgier, Słowenii, Francji, Hiszpanii, Maroka, a także przedstawiciele Komisji Europejskiej, instytutów badawczych oraz szkół wyższych.

18. SPOTKANIE GRUPY PAŃSTW EUROPY ŚRODKOWEJ I WSCHODNIEJ, SARAJEWO, 11-12.05.2016

W dniach 11-12 maja 2016 r. W Sarajewie przedstawiciele Generalnego Inspektora Ochrony Danych Osobowych wzięli udział w 18. Spotkaniu Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA). Gospodarzem tegorocznego wydarzenia była Agencja Ochrony Danych Osobowych w Bośni i Hercegowinie. Wśród uczestników spotkania znaleźli się przedstawiciele 16 organów ochrony danych z następujących krajów: Albanii, Bośni i Hercegowiny, Bułgarii, Chorwacji, Czarnogóry, Federacji Rosyjskiej, Gruzji, Kosowa, Macedonii, Mołdawii, Polski, Republiki Czeskiej, Serbii, Słowacji, Słowenii, Węgier oraz przedstawiciel Rady Europy.

Sesje tematyczne pierwszego dnia spotkania dotyczyły kwestii wideo-nadzoru w sektorze publicznym i prywatnym oraz zagadnieniom przetwarzania szczególnych kategorii danych osobowych przez instytucje opieki zdrowotnej, ochronie praw osób, których dane dotyczą oraz ochronie danych osobowych w sektorze publicznym. W drugim dniu spotkania skupiono się na kwestii zbierania i przetwarzania danych biometrycznych oraz zagadnieniu transgranicznego przekazywania danych i środków ochrony stosowanych przy przetwarzaniu danych osobowych w różnych krajach. W trakcie Spotkania przyjęto Deklarację w sprawie nowego członka Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, na mocy której w poczet członków Grupy przyjęto Agencję Ochrony Danych Osobowych Armenii.

Została podjęta również decyzja, że 19 spotkanie CEEDPA odbędzie się w 2017 r. W Gruzji.

38. MIĘDZYNARODOWA KONFERENCJA RZECZNIKÓW OCHRONY DANYCH OSOBOWYCH i PRYWATNOŚCI, MARRAKESZ, 17-20.10.2016

Międzynarodowe Konferencje to najważniejsze spotkania poświęcone zagadnieniom ochrony danych osobowych i prywatności. W konferencjach odbywających się cyklicznie od 38 lat 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 oraz przedstawiciele biznesu.

Najbardziej istotną, z perspektywy działań polskiego Generalnego Inspektora Ochrony Danych Osobowych, była sesja poświęcona edukacji cyfrowej, podczas której omówiono inicjatywy w tym zakresie ze wszystkich pięciu kontynentów, w tym inicjatywy edukacyjne GIODO. **Polski organ ochrony danych był także współautorem przyjętej podczas Konferencji rezolucji dotyczącej cyfrowej edukacji.**

Tradycyjnie w pierwszych dwóch dniach konferencji odbyła się sesja zamknięta, przeznaczona wyłącznie dla rzeczników ochrony danych i prywatności, dająca im możliwość wymiany doświadczeń i omówienia kluczowych tematów z zakresu ochrony danych. Tegoroczna dyskusja poświęcona była przede wszystkim wyzwaniom dla prywatności, przed jakimi stoją rzecznicy w obliczu dynamicznego rozwoju nowoczesnych technologii. Coraz bardziej zaawansowane usługi i narzędzia informatyczne zmieniają otaczającą nas rzeczywistość, kreując świat coraz bardziej zautomatyzowany. Świat przyszłości, w którym to maszyny podejmują decyzje za nas – jak chociażby wtedy, kiedy decyzje dotyczące naszego ubezpieczenia czy kredytu uwarunkowane są przeprowadzonym przez komputer profilowaniem. Główne zagadnienia poruszane podczas sesji zamkniętej dotyczyły zatem **sztucznej inteligencji, robotyki i szyfrowania**.

W dniach 19-20 października 2016 r. odbyła się sesja otwarta 38. Międzynarodowej Konferencji. Wśród tematów będących przedmiotem dyskusji znalazły się: **ochrona danych i prywatności jako siła napędowa zrównoważonego rozwoju; rozważania na temat tego, jak pogodzić kwestie bezpieczeństwa i prywatności; trendy w technologii i nauce oraz ich wpływ na prywatność, jak również edukacja cyfrowa.**

7. MIĘDZYNARODOWA KONFERENCJA O OCHRONIE DANYCH OSOBOWYCH, MOSKWA, 7-8.11.2016

Przedstawiciel Generalnego Inspektora Ochrony Danych Osobowych wygłosił prezentację na temat inicjatyw edukacyjnych GIODO skierowanych do dzieci.

KONFERENCJA RADY EUROPY, TBILISI, 14-15.12.2016

W dniach 14 – 15 grudnia 2016 r. W Tbilisi (Gruzja) odbyła się konferencja dotycząca wzmacniania ochrony danych osobowych w państwach Partnerstwa Wschodniego organizowana w ramach "Programmatic Cooperation Framework" (PCF). Podstawowym celem tego programu jest wzmacnianie i przyspieszanie procesu wdrażania krajowych reform ochrony danych, tak aby dostosować prawo krajowe do standardów Unii Europejskiej i Rady Europy.

MIĘDZYNARODOWE WARSZTATY NT. OCHRONY DANYCH OSOBOWYCH W OBSZARZE AKTYWNYCH PROGRAMÓW RYNKU PRACY, WARSZAWA, 16.05.2016

„Międzynarodowe doświadczenia w zakresie wykorzystania i ochrony administracyjnych

danych osobowych" – to tytuł warsztatów zorganizowanych w Warszawie przez Ministerstwo Rozwoju i Bank Światowy. Wymiana doświadczeń w odniesieniu do zapewnienia bezpieczeństwa danym osobowym wykorzystywanym przez administrację publiczną, w szczególności zaś możliwości oceny aktywnych programów rynku pracy dzięki wykorzystaniu danych administracyjnych, były głównym celem tego międzynarodowego warsztatu. Generalny Inspektor Ochrony Danych Osobowych oraz jego przedstawiciel przedstawili zagadnienia dotyczące prawnych uwarunkowań wykorzystania danych indywidualnych w celu ewaluacji polityki zatrudnienia w Polsce, podkreślając konieczność przeglądu dotychczasowych ram prawnych w zakresie funkcjonowania rejestrów publicznych, a także przekazywania i wymiany danych osobowych w ramach różnego rodzaju programów badawczych prowadzonych przy udziale wielu instytucji sektora publicznego.

WARSZTATY NA TEMAT IDENTYFIKACJI ELEKTRONICZNEJ, WARSZAWA, 16.09.2016

W dniu 16 września 2016 r. przedstawiciele GIODO uczestniczyli w warsztatach na temat identyfikacji elektronicznej, zorganizowanych w Ministerstwie Cyfryzacji wspólnie z przedstawicielami Komisji Europejskiej. Głównym tematem szkolenia były przepisy rozporządzenia eIDAS w kontekście programu CEF, w szczególności kwestie związane z notyfikacją, zarządzaniem i naruszeniami bezpieczeństwa oraz współpraca państw członkowskim w tym obszarze. Omówiony także został obecny i planowany system identyfikacji elektronicznej w Polsce.

WARSZTATY ROZPATRYWANIA SPRAW, CZARNOGÓRA, 13-14.10.2016

Dominującym tematem Warsztatów było zagadnienie monitoringu wizyjnego. Zwrócono uwagę, że wiele krajów reprezentowanych podczas Warsztatów, opiera swoje działania na przepisach szczególnych dotyczących działalności określonych służb czy wydarzeń (np. sportowych), albo ustawach o ochronie danych osobowych. Widoczny jest też dynamiczny rozwój systemów monitoringu i coraz częstsze jego stosowanie przez podmioty prywatne, co sprzyja sytuacjom konfliktowym i przekłada się na wzrost liczby skarg oraz postępowań, które wg części organów (Wielka Brytania) angażują zbyt duże środki osobowe i organizacyjne.

Wśród innych tematów prezentacji uczestników Warsztatów wymienić należy: metody działania w sprawach realizacji praw podmiotu danych w przypadku prowadzenia wobec niego śledztw, postępowań administracyjnych i dyscyplinarnych, prowadzenie postępowań w sprawie usuwania wyników wyszukiwania, realizacja obowiązku notyfikacji naruszeń danych, transfer danych do państw trzecich, potrzeba regulacji działalności detektywów, skargi na działalność instytucji finansowych i sprzedawców e-commerce oraz aplikacje medyczne.

Tematem wystąpienia przedstawiciela GIODO była nowa procedura rozpatrywania skarg pod rządami unijnego rozporządzenia o ochronie danych osobowych.

V. WYZWANIA

Dynamiczny rozwój nowych technologii to niezmienne wyzwanie dla ochrony danych osobowych.

Największe wyzwania jakie mogą stać przed organem do spraw ochrony danych w kolejnych latach dotyczą wdrażania i upowszechniania nowych technologii. Rozwój ten następuje zarówno w obszarze doskonalenia i powstawania nowych rozwiązań sprzętowych, jak i nowych technologii przetwarzania informacji. Przykładem rozwoju technologii sprzętowej są różnego rodzaju mikro kamery i mikro czujniki wyposażane w elementy łączności bezprzewodowej z innymi urządzeniami np. czujniki mierzące poziom cukru wbudowane w soczewki kontaktowe komunikujące się ze smartfonem, który po przekroczeniu określonego poziomu może sygnalizować ten fakt osobie, której dotyczą w celu podjęcia odpowiednich działań. W przypadku wykrycia poziomu zagrażającego życiu może poinformować np. służby ratunkowe. Przykładem zaś rozwoju technologii przetwarzania **jest oprogramowanie umożliwiające np. rozpoznanie stanów emocjonalnych osoby na podstawie analizy obrazu z kamery systemu monitoringu** czy profilowanie osoby na podstawie danych zbieranych z urządzeń, które bez jej wiedzy mogą być pobierane przez różnego rodzaju czujniki rozmieszczane w galeriach handlowych, muzeach, czy innych miejscach publicznych z urządzeń przenośnych typu telefon komórkowy, tablet czy smartwatch, które dana osoba nosi przy sobie. W praktyce najczęściej dochodzi do ścisłej współpracy różnych rozwiązań nowych technologii z obydwu wymienionych obszarów co stwarza ogromne możliwości pozyskiwania i przetwarzania danych osobowych. Upowszechnienie się rozwiązań technologicznych takich jak aplikacje mobilne, urządzenia elektroniczne wbudowywane w odzież (wearables computing), urządzenia do łączności elektronicznej i przekazywania danych wbudowywane w przedmioty najbliższego otoczenia, Internet rzeczy (IoT – Internet of Things), elektroniczne mierniki transmisja danych typu WiFi, Bluetooth, NFC, zaawansowane metody przetwarzania typu Data mining, BigData, Blockchain i inne, mają coraz większy wpływ na to jak osoba fizyczna funkcjonuje we współczesnym świecie co z kolei przekłada się na ryzyko naruszania praw i wolności tej osoby.

W kontekście ryzyka naruszenia prawa i wolności osób warto zwrócić uwagę na dynamicznie rozwijający się rynek urządzeń określanych jako **internet rzeczy (IoT). W**g raportu Gartnera szacuje się że liczba urządzeń IoT podłączonych do sieci Internet w 2020 wzrośnie z obecnie podłączonych około 6 mld urządzeń do poziomu 21 mld w roku 2020. Istotne

w tym jest to, że IoT podobnie jak wiele innych dynamicznie rozwijających się technologii, technologia ta jest niedojrzała pod względem bezpieczeństwa o czym świadczy szereg skutecznie przeprowadzonych ataków DDoS (Distributed Denial of Service) przeprowadzonych przy użyciu urządzeń IoT takich jak żarówki czy czajniki wyposażone w elementy IoT sterowania przy użyciu sieci WiFi. Jak twierdzą specjaliści problem bezpieczeństwa urządzeń IoT jest skomplikowany z uwagi na konieczność stosowania zabezpieczeń w warstwie aplikacyjnej, sprzętowej, sieciowej, komunikacyjnej i analitycznej co w systemach heterogenicznych jest trudne z powodu braku jednolitych i powszechnie stosowanych standardów w tym zakresie. Stąd zagadnienia bezpieczeństwa trzeba będzie uwzględniać podczas przeprowadzania oceny skutków stosowania tych technologii na ochronę prywatności do czego zobowiązywać będą od 25 maja 2018 r. nowe regulacje zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/EW (RODO).

Nowe prawo, mając na uwadze zagrożenia dla ochrony prywatności wynikające z zastosowań nowych technologii wprowadza w niektórych okolicznościach obowiązek stosowania nowych środków ochrony. Należą do nich między innymi środki organizacyjne takie jak wprowadzenie **zasady uwzględniania ochrony danych w fazie projektowania, domyślnej ochrony danych, czy obowiązku przeprowadzenia oceny skutków** zastosowania określonej technologii na ochronę prywatności. Ma to niebagatelne znaczenie w kontekście tworzenia aplikacji mobilnych, Internetu rzeczy czy systemów teleinformatycznych tworzonych chociażby w interesie publicznym (których beneficjentami są tysiące a nawet miliony osób fizycznych). Monitorowanie stanu wiedzy technicznej w zakresie zasad i środków bezpieczeństwa jest jednym z głównych obszarów zainteresowania Departamentu Informatyki. Ogromne znaczenie w tym zakresie mają normy techniczne wydawane w tym zakresie przez organizacje międzynarodowe takie jak ISO (International Organization for Standardization), IEC (International Electrotechnical Commission), które są organizacjami międzynarodowymi oraz organizacje Europejskie takie jak CEN (European Committee for Standardization) oraz CENELEC (European Committee for Electrotechnical Standardization). W zakresie komunikacji elektronicznej i jej bezpieczeństwa ogromne znaczenie mają z kolei normy wydawane przez ETSI (European Telecommunications Standards Institute). Coraz większe znaczenie w zakresie rozpowszechniania wiedzy w zakresie dobrych praktyk i bezpieczeństwa informacji mają ponadto opracowania i publikacje wydawane przez ENISA (Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji). Dla zapewnienia właściwego poziomu bezpieczeństwa duże znaczenie mają ponadto normy i praktyki dotyczące zarządzania bezpieczeństwem oraz kontroli i monitorowania tych procesów. Najnowszy stan wiedzy w tym zakresie również zawarty jest w normach publikowanych wspólnie przez ISO i IEC oraz dobrych praktykach i metodykach publikowanych przez międzynarodowe organizacje audytorskie takie jak IIA (The Institute of Internal Auditors) oraz ISACA (Międzynarodowe Stowarzyszenie Audytorów Systemów Informatycznych).

Wraz z końcem 2016 roku w świecie nowych technologii pojawiły się nowe zjawiska, które z uwagi na ich charakter, w sposób szczególny mogą wpłynąć na prywatność i wolność

osób, w tym przetwarzanie danych osobowych. Jednym z nich jest tzw. **cartapping** polegający na śledzeniu samochodów w oparciu o zamontowane w nich technologie służące do komunikacji i wymiany danych z otoczeniem. Pośredni związek z tym zjawiskiem może mieć ogólnoeuropejski system szybkiego powiadamiania o wypadkach drogowych (eCall - Rozporządzenie 2015/758). Nowe obowiązki nakładane na producentów samochodów od marca 2018 r. mogą być pokusą do montowania dodatkowych zaawansowanych technologii ingerujących w prywatność podróżujących nimi osób.

Dotychczasowe pytania o wyjaśnienia i opinie kierowane do GIODO wskazują na rosnącą popularność aplikacji mobilnych oraz mobilnych i stacjonarnych urządzeń pomiarowych, z którymi nierozerwalnie wiążą się takie technologie transmisji danych jak Bluetooth czy WiFi. Szczególne miejsce zajmują tutaj rozwiązania dotyczące **przetwarzania danych o aktywności i stanie zdrowia osób korzystających z urządzeń mobilnych** wyposażonych w czujniki do pomiaru takich parametrów jak np. tętno, ciśnienie krwi, liczba przebytych kroków, szybkość przemieszczania się, zużyta energia itp. Tematyką przetwarzania danych wrażliwych o stanie zdrowia przy użyciu aplikacji mobilnych zajęła się w ostatnim okresie również podgrupa ds. e-government Grupy Roboczej art. 29. Do podgrupy tej przekazano do zaopiniowania przygotowywany w ramach Komisji europejski kodeks dobrych praktyk dla twórców rozwiązań mobilnych w zakresie zbierania, analizy i przekazywania danych medycznych tzw. mobile health.

Dynamicznie zmieniające się technologie komunikacji elektronicznej oraz powstałe w ich wyniku luki w prawie mającym zapewnić prywatność i ochronę danych osobowych w sektorze łączności elektronicznej, zmusiły pod koniec ubiegłego roku do przedstawienia przez Komisję Europejską propozycji nowego aktu prawnego w tym zakresie. Jest nim projekt rozporządzenia uchylającego dyrektywę 2002/58/EC i wprowadzającego nowe zasady odnoszące się do ochrony poufności komunikacji i danych osobowych w sektorze komunikacji elektronicznej. w projekcie tym bezpośrednio wskazano, że organami w państwach członkowskich odpowiedzialnymi za jej stosowanie mają być te same organy, które powołane zostały do monitorowania stosowania RODO. w związku z tym GIODO zamierza ponownie przyjrzeć się mechanizmom związanym z profilowaniem osób za pomocą informacji przechowywanych na urządzeniach użytkowników (m.in. W plikach cookie) oraz pośrednim rozwiązaniom w tym zakresie takim jak coraz bardziej popularna, wbudowywana w przeglądarki internetowe technologia DoNotTrack, której zasady i odnoszące się do niej standardy opracowane zostały przez World Wide Web Concortium (W3C) – organizację międzynarodowa zajmującą się ustanawianiem standardów pisania stron i aplikacji internetowych (WWW). W tym miejscu warto również wspomnieć o wątpliwościach jakie wzbudzała w ostatnim czasie polityka prywatności realizowana przez firmę Microsoft w zakresie danych zbieranych przez system operacyjny Windows 10. Przełom roku 2016/2017 przyniósł nowe deklaracje twórców tego systemu w zakresie oczekiwań użytkowników oraz realizacji żądań europejskich organów ochrony danych w zakresie dostosowania go do wymaganych standardów ochrony danych w UE.

Wspomniane na początku obszary technologiczne można również sprowadzić do wspólnego mianownika jakim jest sztuczna inteligencja. Zastosowanie robotów i coraz częściej i szerzej stosowana autonomia ich działania, zachęca do dyskusji na temat standardów zarówno technologicznych jak i etycz-

nych w tym zakresie. Temat ten nie ominął zainteresowania organów Unii Europejskiej. Ich wynikiem jest przyjęte w dniu 12 stycznia 2017 roku sprawozdanie Komisji Parlamentu Europejskiego ds. prawnych, w którym zasygnalizowano potrzebę uregulowania statusu i odpowiedzialności robotów i innych autonomicznie działających urządzeń. Komisja ta zaproponowała wprowadzenie do przepisów prawa pojęcia „osoby elektronicznej" obok „osoby fizycznej" oraz „osoby prawnej". Komisja ta przedstawiła również koncepcję wypracowania kodeksu dobrych praktyk, który miałby obejmować społeczne, środowiskowe i zdrowotne problemy związane z oddziaływaniem robotów. W przyjętym sprawozdaniu za roboty uznaje się urządzenia posiadające formę fizyczną, wyposażone w czujniki i połączone z otoczeniem w taki sposób, że mogą wymieniać dane. Zapowiedziano również, że kolejna generacja robotów może obejmować urządzenia o coraz większej zdolności do samokształcenia się (autonomiczne auta, roboty medyczne, drony, roboty dla użytkowników domowych, roboty przemysłowe, zabawki, roboty w przemyśle rolniczym). W raporcie zwraca się uwagę, że w wielu obszarach postęp technologiczny eliminuje pośrednio czynnik ludzki w procesie przetwarzania danych, z uwagi na możliwość podejmowania autonomicznych decyzji przez roboty. To z kolei wymaga określenia odpowiednich zasad współdziałania, w tym określenia obowiązków i odpowiedzialności, zarówno dla twórców takich robotów, jak i prawa i zadania osób, których dane osobowe mogą być w ten sposób przetwarzane.

VI. 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	Podmiot, do którego wystąpienie było skierowane	Data i sygnatura sprawy	Przedmiot
1.	Ministerstwo Sprawiedliwości	2016-03-08 DOLiS-035-637/16	Wystąpienie z art. 19a ust. 2 u.o.d.o. do Ministra Sprawiedliwości z prośbą o podjęcie działań dotyczących skierowania do organów samorządu komorniczego informacji o konieczności respektowania powszechnie obowiązujących przepisów prawa w zakresie ograniczeń dostępu do informacji o majątku osoby fizycznej
2.	Urząd Miasta Krakowa	2016-04-01 DOLiS-035-2332/15	Wystąpienie z art. 19a ust. 1 u.o.d.o. kierowane do Prezydenta Miasta Krakowa w związku z pozyskiwaniem szerokiego zakresu danych na formularzu wniosku o udostępnienie informacji publicznej.
3.	Urząd Gminy Legnickie Pola	2016-05-10 DOLiS-035-1170/16	Wystąpienie z art. 19a ust. 1 u.o.d.o. kierowane do Wójta Gminy Legnickie Pola związane z opublikowaniem

			w szerokim zakresie dane osobowe osób fizycznych z załącznika do uchwały Rady Gminy.
4.	Ministerstwo Edukacji Narodowej	2016-06-23 DOLiS-035-1624/16	Wystąpienie z art. 19a ust. 2 u.o.d.o. kierowane do Ministra Edukacji Narodowej o podjęcie prac legislacyjnych w celu uregulowania zasad monitorowania losów absolwentów po ukończeniu gimnazjów.
5.	Polski Związek Działkowców	2016-07-19 DOLiS-035-1174/16	Wystąpienie z art. 19a ust. 1 u.o.d.o. kierowane do Polskiego Związku Działkowców o podjęcie działań mających na celu dostosowanie procesu przetwarzania danych osobowych do wymogów określonych przepisami ustawy o ochronie danych osobowych.
6.	Ministerstwo Finansów	2016-07-20 DOLiS-033-152/16	Wystąpienie z art. 19a ust. 2 u.o.d.o. do Ministra Zdrowia z wnioskiem o rozważenie wprowadzenia do ustawy o obrocie instrumentami finansowymi zmian dotyczących ustawowego uregulowania zasad ochrony pracowników w przypadku zgłaszania przez nich nieprawidłowości związanych z funkcjonowaniem firmy inwestycyjnej
7.	Urząd Miasta Płock	2016-08-04 DOLiS-035-1759/16	Wystąpienie z art. 19a ust. 1 u.o.d.o. kierowane do Prezydenta Miasta Płocka w związku z praktyką o rozsyłania korespondencji w formie obejmującej rozdzielnik zawierający dane osobowe w postaci imion i nazwisk oraz adresów.
8.	Ministerstwo Zdrowia	2016-08-19 DOLiS-035-924/16	Wystąpienie z art. 19a ust. 2 u.o.d.o. do Ministra Zdrowia o podjęcie prac legislacyjnych mających na celu uregulowanie kwestii przetwarzania danych o stanie zdrowia w związku z prowadzeniem profilaktyki

			zdrowotnej lub realizacją programów zdrowotnych albo programów polityki zdrowotnej, w tym stworzenie właściwych podstaw prawnych funkcjonowania Systemu Informatycznego Monitorowania Profilaktyk.
9.	Ministerstwo Sprawiedliwości	2016-09-13 DOLiS-035-1732/16	Wystąpienie z art. 19a ust. 2 u.o.d.o. do Ministra Sprawiedliwości o podjęcie prac legislacyjnych mających na celu uregulowanie kwestii przetwarzania danych osobowych przez opiniodawcze zespoły sądowe specjalistów oraz dostępu do tych danych przez osoby badane.
10.	Urząd Gminy Gowo-rowo	2016-09-13 DOLiS-035-2239/16	Wystąpienie z art. 19a ust. 1 u.o.d.o. do Wójta Gminy Goworowo w związku z pozyskaniem informacji o tym, że za pośrednictwem deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, zbierany jest szeroki zakres informacji na temat mieszkańców gminy
11.	Urząd Gminy w Wyrykach	2016-11-22 DOLiS-035-2141/16	Wystąpienie z art. 19a ust. 1 u.o.d.o. do Wójta Gminy w Wyrykach w związku z praktyką żądania od osób ubiegających się o zatrudnienie „zaświadczenia wystawionego przez lekarza medycyny pracy o stanie zdrowia pozwalającym na wykonywanie czynności objętych zakresem zadań stanowiska pracy”
12.	Ministerstwo Rodziny Pracy i Polityki Społecznej	2015-12-22 DOLiS-035-2141/16	Wystąpienie z art. 19a ust. 2 u.o.d.o. do Ministra Rodziny, Pracy i Polityki Społecznej o podjęcie prac legislacyjnych mających na celu zmianę przepisów rozporządzenia 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.
13.	Minister Spraw Wewnętrznych i Administracji	26.08.2016 DIS-76298/16	Wystąpienie w sprawie podjęcie inicjatywy ustawodawczej w celu zmiany przepisów dotyczących ewidencji gruntów i budynków w zakresie jawności numeru księgi wieczystej.
14.	Minister Spraw Wewnętrznych i Administracji	12.08.2016 DIS-K-421/66/15/72796/16	Wystąpienie w sprawie rozważenia potrzeby podjęcia inicjatywy ustawodawczej w celu zmiany przepisów dotyczących uprawnienia Szefa Urzędu do Spraw Cudzoziemców do dokonywania wpisów danych VIS – wynikającego z art. 5 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.).

Załącznik nr 2

Wykaz kontroli przeprowadzonych w 2016 r.

Lp.	Data i sygnatura kontroli	Podmiot i miejsce kontroli	Inicjatywa kontroli	Rozstrzygnięcie
1.	12.01.2016 DIS-K-421/1/16	Lex Superior Sp. Z o.o., Warszawa, ul. Stawki 2	Departament Orzecznictwa Legislacji i Skarg	
2.	11-15.01.2016 DIS-K-421/2/16	Publiczna Szkoła Podstawowa Stowarzyszenia Rozwoju Wsi, Jarnołtówek 109	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
3.	11-15.01.2016 DIS-K-421/3/16	Stowarzyszenie Rozwoju Wsi, Jarnołtówek 109	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
4.	11-15.01.2016 DIS-K-421/4/16	Ministerstwo Zdrowia, Warszawa, ul. Miodowa 15	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
5.	11-13.01.2016 DIS-K-421/5/16	Komenda Stołeczna Policji, Warszawa, ul. Nowolipie 2	z urzędu	ustalenia przekazano Komendantowi Głównemu Policji
6.	13-15.01.2016 DIS-K-421/6/16	Komenda Główna Policji, Warszawa, ul. Puławska 148/150	z urzędu	
7.	14-15.01.2016 DIS-K-421/7/16	Wit Wach Usługi Ogólnobudowlane, Warszawa, ul. Odyńca 9	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
8.	13-15.01.2016 DIS-K-421/8/16	Centrum Systemów Informacyjnych	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji

		Ochrony Zdrowia, Warszawa, ul. Dubois 5A		
9.	18-19.01.2016 DIS-K-421/9/16	NTE Sp. Z o.o., Warszawa, ul. Serocka 8/3	Zespół ds. Egzekucji Administracyjnej	pismo informujące do Zespołu ds. Egzekucji Administracyjnej
10.	18-22.01.2016 DIS-K-421/10/16	Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości, Łomża, ul. Akademicka 14	Departament Orzecznictwa Legislacji i Skarg	ustalenia przekazano do Komendy Miejskiej Policji w Łomży
11.	25-29.01.2016 DIS-K-421/11/16	Koleje Mazowieckie – KM Sp. Z o.o., Warszawa, ul. Lubelska 26	z urzędu	nie stwierdzono uchybień
12.	25-29.01.2016 DIS-K-421/12/16	Szpital Wojewódzki im. Prymasa Kardynała Stefana Wyszyńskiego, Sieradz, ul. Armii Krajowej 7	Prokuratura Rejonowa w Sieradzu	decyzja GIODO
13.	26-29.01.2016 DIS-K-421/13/16	Mazowiecki Urząd Wojewódzki w Warszawie, Warszawa, pl. Bankowy 3/5	z urzędu	nie stwierdzono uchybień
14.	01-05.02.2016 DIS-K-421/14/16	Zarząd Komunikacji Miejskiej w Gdyni, Gdynia, ul. Zakręt do Oksywia 10	z urzędu	decyzja GIODO
15.	01-06.02.2016 DIS-K-421/15/16	Black Dot Sp. Z o.o., Gdańsk, ul. Norwida 2 lok. 211	w związku z kontrolą DIS-K-421/1/16	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg

16.	02-05.02.2016 DIS-K-421/16/16	Silesia Izba Handlowa Sp. Z o.o., Wrocław, al. Karkonoska 8 lok. 409	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
17.	02-04.02.2016 DIS-K-421/17/16	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
18.	08-10.02.2016 DIS-K-421/18/16	Info Veriti Polska Sp. Z o.o. Obsługa Serwisu Internetowego sp. j., Warszawa, ul. Serwituty 23	w związku z kontrolą DIS-K-421/204/09	materiał dowodowy przekazano do sprawy DIS-K-421/204/09
19.	08-12.02.2016 DIS-K-421/19/16	Starostwo Powiatowe w Cieszynie, Cieszyn, ul. Bobrecka 29	z urzędu	decyzja GIODO
20.	15-19.02.2016 DIS-K-421/20/16	Euronet Norbert Saniewski sp. j., Białystok, ul. Upalna 5A lok. 10	Urząd Komunikacji Elektronicznej	usunięto uchybienia
21.	17-19.02.2016 DIS-K-421/22/16	Urząd ds. Cudzoziemców, Warszawa, ul. Koszykowa 16	Departament Edukacji Społecznej i Współpracy Międzynarodowej	nie stwierdzono uchybień
22.	22-24.02.2016 DIS-K-421/23/16	Urząd Kontroli Skarbowej w Poznaniu, Poznań, ul. Strzelecka 2/6	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji

23.	29.02-04.03.2016 DIS-K-421/24/16	Urząd Miasta Bydgoszczy, Bydgoszcz, ul. Jezuicka 1	z urzędu	nie stwierdzono uchybień
24.	29.02-04.03.2016 DIS-K-421/25/16	Has Project Sp. Z o.o., Mosina, ul. Ogrodowa 12A	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
25.	29.02-04.03.2016 DIS-K-421/26/16	Gminny Ośrodek Pomocy Społecznej w Drużbicach, Drużbice 20,	Departament Rejestracji	nie stwierdzono uchybień
26.	02-03.03.2016 DIS-K-421/27/16	Toyota Logistics Services Poland Sp. Z o.o., Warszawa, ul. Poleczki 23	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
27.	02.03.2016 DIS-K-421/28/16	DBMS Sp. Z o.o., Warszawa, ul. Gwiaździsta 71	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
28.	07-11.03.2016 DIS-K-421/29/16	UPC Polska Sp. Z o.o., Warszawa, Al. Jana Pawła II 27	z urzędu	decyzja GIODO
29.	07-11.03.2016 DIS-K-421/30/16	Starostwo Powiatowe w Mławie, Mława, ul. Reymonta 6	z urzędu	decyzja GIODO
30.	07-11 i 14-15.03.2016 DIS-K-421/31/16	Kreditech Polska Sp. Z o.o., Warszawa, ul. Prosta 32	z urzędu	
31.	14.03.2016 DIS-K-421/32/16	Authalia.com Sp. Z o.o., Olsztynek, ul. Jana Pawła II 9	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
32.	14-18.03.2016 DIS-K-421/33/16	Starostwo Powiatowe w Wołominie, Wołomin, ul. Prądzyńskiego 3	z urzędu	decyzja GIODO

33.	14-18.03.2016 DIS-K-421/40/16	Nadbużański Oddział Straży Granicznej, Chełm, ul. Trubakowska 2	z urzędu	przywrócono stan zgodny z prawem
34.	21-25.03.2016 DIS-K-421/47/16	Starostwo Powiatowe w Chełmie, Chełm, Pl. Niepodległości 1	z urzędu	decyzja GIODO
35.	21-25.03.2016 DIS-K-421/48/16	Grupa Allegro Sp. Z o.o., Poznań, ul. Grunwaldzka 182	z urzędu	nie stwierdzono uchybień
36.	21-25.03.2016 DIS-K-421/49/16	Rapid Finance Polska Sp. Z o.o., Warszawa, ul. Postępu 18A	Prokuratura Rejonowa w Opolu	decyzja GIODO
37.	18.03.2016 DIS-K-421/51/16	Filip Hamerla prowadzący działalność gospodarczą pod nazwą Eventroom Filip Hamerla, Warszawa, ul. Stawki 2	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
38.	29.03-01.04.2016 DIS-K-421/52/16	Marszałek Województwa Mazowieckiego, Warszawa, ul. Jagiellońska 26	z urzędu	nie stwierdzono uchybień
39.	04-06.04.2016 DIS-K-421/53/16	Zarząd Transportu Miejskiego w Warszawie, Warszawa, ul. Żelazna 61	Zespół ds. Egzekucji Administracyjnej	wnioski przekazano do Zespołu ds. Egzekucji Administracyjnej
40.	11-15.04.2016 DIS-K-421/54/16	Komenda Powiatowa Policji w Wieliczce, Wieliczka, ul. Jedynaka 30a	z urzędu	przywrócono stan zgodny z prawem
41.	11-15.04.2016 DIS-K-421/55/16	Nutricus Sp. Z o.o., Warszawa, Al. Jana Pawła II 61 lok. 311	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji

42.	11.04.2016 DIS-K-421/56/16	Egi.pl Sp. Z o.o., Warszawa, ul. Stawki 2	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
43.	12-15.04.2016 DIS-K-421/57/16	ASEC S.A., Kraków, ul. Olszańska 5	w związku z kontrolą DIS-K-421/204/09	nie stwierdzono uchybień
44.	18-22.04.2016 DIS-K-421/58/16	Starostwo Powiatowe w Nowym Dworze Maz., Nowy Dwór Maz., ul. Paderewskiego 1B	z urzędu	decyzja GIODO
45.	18-22.04.2016 DIS-K-421/59/16	Politechnika Świętokrzyska, Kielce, Al. Tysiąclecia Państwa Polskiego 7	z urzędu	nie stwierdzono uchybień
46.	18-21.04.2016 DIS-K-421/60/16	Starostwo Powiatowe w Węgrowie, Węgrów, ul. Przemysłowa 5	z urzędu	przywrócono stan zgodny z prawem
47.	18-22.04.2016 DIS-K-421/61/16	Starostwo Powiatowe w Piasecznie, Piaseczno, ul. Chyliczkowskiej 14	z urzędu	decyzja GIODO
48.	25-29.04.2016 DIS-K-421/66/16	SP ZOZ Szpital Wojewódzki im. Mikołaja Kopernika, Koszalin, ul. Chałbińskiego 7	Rzecznik Praw Pacjenta	nie stwierdzono uchybień
49.	25-29.04.2016 DIS-K-421/67/16	Starostwo Powiatowe w Puławach, Puławy, Al. Królewska 19	z urzędu	przywrócono stan zgodny z prawem
50.	25-29.04.2016 DIS-K-421/68/16	Platinium Wellness Sp. Z o.o., Kraków, ul. Lea 116	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO

51.	25-29.04.2016 DIS-K-421/69/16	Komenda Powiatowa Policji w Otwocku, Otwock, ul. Pułaskiego 7a	z urzędu	nie stwierdzono uchybień
52.	09-13.05.2016 DIS-K-421/75/16	Starostwo Powiatowe w Malborku, Malbork, Pl. Słowiański 17	z urzędu	decyzja GIODO
53.	09-13.05.2016 DIS-K-421/76/16	Starostwo Powiatowe w Stargardzie, Stargard, ul. Skarbowa 1	z urzędu	decyzja GIODO
54.	09-13.05.2016 DIS-K-421/78/16	Vivus Finance Sp. Z o.o., Warszawa, ul. 17 Stycznia 56	z urzędu	decyzja GIODO
55.	11-13.05.2016 DIS-K-421/79/16	Samodzielny Zespół Publicznych Zakładów Lecznictwa Otwartego Warszawa - Ochota, Warszawa, ul. Szczęśliwicka 36	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
56.	16-20.05.2016 DIS-K-421/80/16	Gotówkomat Polskie Płatności Sp. Z o.o., Warszawa, ul. Płocka 5A	w związku z kontrolą DIS-K-421/124/15	nie stwierdzono uchybień
57.	16-20.05.2016 DIS-K-421/81/16	Wydział Konsularny Ambasady RP w Sofii, ul. Chan Krum 46	z urzędu	usunięto uchybienia
58.	16-20.05.2016 DIS-K-421/82/16	Urząd Miasta i Gminy Witnica, ul. KRN 6	Komenda Miejska Policji w Gorzowie Wlkp.	decyzja GIODO
59.	30.05-01.06.2016 DIS-K-421/83/16	Ruch S.A., Warszawa, ul. Chłodna 52	w związku z kontrolą DIS-K-421/124/015	nie stwierdzono uchybień

60.	18-24.05.2016 DIS-K-421/84/16	Przemysław Zegarek prowadzący działalność gospodarczą pod nazwą „Lex Artist Przemysław Zegarek”, Warszawa, ul. Szańcowa 74 lok. 1	z urzędu	decyzja GIODO
61.	23-25.05.2016 DIS-K-421/85/16	Toyota Bank Polska S.A., Warszawa, ul. Postępu 18B	w związku ze sprawdzeniem DIS-K-421/45/15/SPR 10	decyzja GIODO
62.	23-25.05.2016 DIS-K-421/86/16	Komenda Wojewódzka Policji w Opolu, ul. Korfantego 2	z urzędu	nie stwierdzono uchybień
63.	30.05-02.06.2016 DIS-K-421/87/16	Przedsiębiorstwo Komunikacji Trolejbusowej Sp. Z o.o., Gdynia, ul. Zakręt do Oksywia 1	w związku z kontrolą DIS-K-421/14/16	decyzja GIODO
64.	30.05-02.06.2016 DIS-K-421/88/16	Powszechna Kasa Oszczędności Bank Polski S.A., Warszawa, ul. Puławska 15	w związku ze sprawdzeniem	decyzja GIODO
65.	02.06.2016 DIS-K-421/89/16	Beata Wolska – Żewuska prowadząca działalność gospodarczą pod nazwą „Skala Beata Ewa Wolska – Żewuska”, Warszawa, ul. Krakowska 239	w związku z kontrolami DIS-K-421/124/15 i DIS-K-421/83/16	nie stwierdzono uchybień
66.	03.06.2016 DIS-K-421/90/16	Michał Osiejewski prowadzący działalność gospodarczą pod	w związku z kontrolami DIS-K-421/124/15	nie stwierdzono uchybień

		nazwą „Michał Osiejewski”, Warszawa, ul. Chłodna 52	i DIS-K-421/83/16	
67.	06-10.06.2016 DIS-K-421/91/16	Pomorska Komunikacja Samochodowa Sp. Z o.o., Gdynia, ul. Hryniewickiego 6c lok. 43	w związku z kontrolą DIS-K-421/14/16	decyzja GIODO
68.	01-03.06.2016 DIS-K-421/92/16	Prezydent m.st. Warszawy, Warszawa, Plac Bankowy 3/5	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
69.	06-10.06.2016 DIS-K-421/93/16	SICK Sp. Z o.o., Warszawa, ul. Nakielska 3	z urzędu	decyzja GIODO
70.	13-17.06.2016 DIS -K- 21/9 4/16	Wydział Konsularny Ambasady RP w Rydze, Mednieku iela 6b	z urzędu	usunięto uchybienia
71.	13-16.06.2016 DIS-K-421/95/16	Orange Polska S.A., Warszawa, Al. Jerozolimskie 160	z urzędu	nie stwierdzono uchybień
72.	20-22.06.2016 DIS-K-421/97/16	AppVerk Sp. Z o.o., Poznań, ul. Zakręt 8	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
73.	20-22.06.2016 DIS-K-421/98/16	Telewizja Kablowa Hajnówka Kiędys, Kiryluk sp. j., Hajnówka, ul. Warszawska 1E	w związku z kontrolą DIS-K-421/20/16	usunięto uchybienia
74.	28.06-04.07.2016 DIS-K-421/99/16	PCG Polska Sp. Z o.o., Warszawa, ul. Piękna 19	z urzędu	nie stwierdzono uchybień

75.	27.06-01.07.2016 DIS-K-421/100/16	Izba Celna w Warszawie, ul. Ciołka 14A	z urzędu	nie stwierdzono uchybień
76.	27.06-01.07.2016 DIS-K-421/101/16	Komenda Wojewódzka Policji w Gdańsku, ul. Okopowa 15	z urzędu	ustalenie przekazano Komendantowi Głównemu Policji
77.	04-08 i 11-12.07.2016 DIS-K-421/102/16	Kancelaria Prawna Skarbiec R. Nogacki sp. k., Warszawa, ul. Maciejki 13	Departament Orzecznictwa Legislacji i Skarg	zawiadomienie o przestępstwie
78.	04-08 i 11-12.07.2016 DIS-K-421/103/16	Portal Skarbiec.biz S.A., Warszawa, ul. Ruchliwa 15	Departament Orzecznictwa Legislacji i Skarg	zawiadomienie o przestępstwie
79.	11-13.07.2016 DIS-K-421/104/16	Jerzy Chamielec prowadzący działalność gospodarczą pod nazwą „Mamacube Jerzy Chamielec”, Grajów 310	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
80.	11-14.07.2016 DIS-K-421/105/16	Polski Klub Ekologiczny w Krakowie Koło Miejskie w Gliwicach, ul. Ks. Ziemowita 1 lok. III P	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
81.	11-15.07.2016 DIS-K-421/106/16	Izba Celna w Olsztynie, ul. Dworcowa 1	z urzędu	nie stwierdzono uchybień
82.	11-15.07.2016 DIS-K-421/107/16	GoGet.pl car sharing Sp. Z o.o., Wrocław, ul. Pieszycka 17	Departament Rejestracji	wnioski przekazano do Departamentu Rejestracji
83.	18-22.07.2016	Izba Celna w Białej Podlaskiej,	z urzędu	nie stwierdzono uchybień

	DIS-K-421/108/16	ul. Celników Polskich 21		
84.	18-22.07.2016 DIS-K-421/109/16	Blue Media S.A., Sopot, ul. Haffnera 6	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
85.	18-22.07.2016 DIS-K-421/110/16	Komenda Wojewódzka Policji w Radomiu, ul. 11-go Listopada 37/59	z urzędu	ustalenia przekazano Komendantowi Głównemu Policji
86.	19-20.07.2016 DIS-K-421/111/16	„Creative Anna Pękowska”, Warszawa, ul. Stawki 2	Departament Orzecznictwa Legislacji i Skarg	
87.	25-27.07.2016 DIS-K-421/112/16	ABC PRO Sp. Z o.o., Warszawa, ul. Owsiana 12	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
88.	25-29.07.2016 DIS-K-421/113/16	Komenda Wojewódzka Policji w Bydgoszczy, ul. Powstańców Wielkopolskich 7	z urzędu	ustalenia przekazano Komendantowi Głównemu Policji
89.	25-29.07.2016 DIS-K-421/114/16	Powiatowy Inspektor Nadzoru Budowlanego w Aleksandrowie Kujawskim, ul. Słowackiego 12	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
90.	01-05.08.2016 DIS-K-421/115/16	SP ZOZ Wojewódzki Szpital Zespolony im. Jędrzeja Śniadeckiego, Białystok, ul. Curie – Skłodowskiej 26	z urzędu	decyzja GIODO
91.	01-05.08.2016 DIS-K-421/116/16	Urząd Celny w Lublinie,	z urzędu	nie stwierdzono uchybień

		ul. Energetyków 20/22		
92.	08-12.08.2016 DIS-K-421/117/16	Specjalistyczna Przychodnia Lekarska dla Pracowników Wojska SP ZOZ, Warszawa, ul. Nowowiejska 31	z urzędu	nie stwierdzono uchybień
93.	16-18.08.2016 DIS-K-421/118/16	Novemedia Ltd Sp. Z o.o. Oddział w Polsce, Inowrocław, ul. Dworcowa 55	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
94.	22-26.08.2016 DIS-K-421/119/16	Urząd Celny w Ciechanowie, ul. Gostkowska 39a	z urzędu	nie stwierdzono uchybień
95.	22-26.08.2016 DIS-K-421/120/16	Towarzystwo Ubezpieczeń i Reasekuracji Allianz Polska S.A., Warszawa, ul. Rodziny Hiszpańskich 1	z urzędu	usunięto uchybienia
96.	22-26.08.2016 DIS-K-421/121/16	Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A., Wrocław, ul. Armii Ludowej 21	z urzędu	
97.	31.08-02.09 i 05-06.09.2016 DIS-K-421/122/16	Netia S.A., Warszawa, ul. Poleczki 13	z urzędu	nie stwierdzono uchybień
98.	01-02 i 05-07.09.2016 DIS-K-421/123/16	Baxter Polska Sp. Z o.o., Warszawa, ul. Kruczkowskiego 8	Departament Rejestracji	decyzja GIODO
99.	05-09.09.2016 DIS-K-421/124/16	Izba Celna w Opolu, ul. Szpitalna 3b-5-7	z urzędu	nie stwierdzono uchybień
100.	15-16.09.2016 DIS-K-421/135/16	Fundacja Rozwoju Edukacji Matematycznej, Warszawa,	z urzędu	nie stwierdzono uchybień

		ul. Brazylijska 9A lok. 46		
101.	12-16.09.2016 DIS-K-421/136/16	Stowarzyszenie „moja Mammografia”, Gdańsk, ul. Widok 26	z urzędu	decyzja GIODO
102.	12-15.09.2016 DIS-K-421/137/16	Polkomtel Sp. Z o.o. Warszawa, ul. Konstruktorska 4	z urzędu	nie stwierdzono uchybień
103.	12-16.09.2016 DIS-K-421/138/16	Agencja Pośrednictwa Pracy TopJob Tadeusz Łańcucki, Gdańsk, ul. Wenus 34	z urzędu	decyzja GIODO
104.	12-16.09.2016 DIS-K-421/139/16	Ministerstwo rolnictwa i Rozwoju Wsi, Warszawa, ul. Wspólna 30	z urzędu	nie stwierdzono uchybień
105.	19-23.09.2016 DIS-K-421/140/16	Urząd Marszałkowski Województwa Dolnośląskiego, Wrocław, ul. Wybrzeże Słowackie 12-14	z urzędu	nie stwierdzono uchybień
106.	19-23.09.2016 DIS-K-421/141/16	Ruch S.A., Warszawa, ul.Chłodna 52	z urzędu	nie stwierdzono uchybień
107.	19-23.09.2016 DIS-K-421/142/16	Szpitala Powiatowy im. Jana Pawła II w Trzciance, Trzcianka, ul. Sikorskiego 9	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
108.	20-23.09.2016 Zmiana 20-22.09.2016 DIS-K-421/143/16	Amicus Legis Kancelaria Prawna Sp.z o.o., Warszawa, ul. Bazyliańska 20	z urzędu	decyzja GIODO
109.	21-23.09.2016 DIS-K-421/144/16	Prezydent Miasta Łodzi, Łódź, ul. Piotrkowska 104	z urzędu	decyzja GIODO

110.	26-30.09.2016 DIS-K-421/150/16	Referat ds. konsularnych Ambasady RP w Budapeszcie, Budapeszt, Varosligeti fasor 16	z urzędu	usunięto uchybienia
111.	27-30.09.2016 i 04-07.10.2016 DIS-K-421/151/16	Komunikacyjny Związek Komunalny Górnośląskiego Okręgu Przemysłowego, Katowice, ul. Barbary 21 a	Pismo UOKiK	
112.	03.07.10.2016 DIS-K-421/152/16	Wydział Konsularny Ambasady RP w Bukareszcie, Bukareszt, Aleea Alexandru 23	z urzędu	usunięto uchybienia
113.	04-07 i 10.10.2016 DIS-K-421/153/16	Jacek Bogiel Komornik Sądowy przy Sądzie Rejonowym dla Warszawy Woli w Warszawie – Kancelaria Komornicza, Warszawa, ul Karolkowa 58A	z urzędu	wszczęcie postępowania administracyjnego
114.	04-07.10.2016 DIS-K-421/154/16	Small Planet Airlines Sp. Z o.o., Warszawa, ul. Krakowiaków 48	Pismo Prezesa ULC	decyzja GIODO
115.	04.07.10.2016 DIS-K-421/155/16	Komunikacyjny Związek Komunalny Górnośląskiego Okręgu Przemysłowego, Katowice, ul. Barbary 21a	Zespół do Spraw Egzekucji Administracyjnej	Wnioski przekazano do Zespołu do Spraw Egzekucji Administracyjnej
116.	10-14.10.2016 DIS-K-421/166/16	Spaczyński, Szczepaniak i Wspólnicy Sp.k., Warszawa, rondo ONZ 1	z urzędu	nie stwierdzono uchybień
117.	11-14.10.2016 DIS-K-421/167/16	Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej, Warszawa, ul. Konstruktorska 3 a	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień

118.	17-21.10.2016 DIS-K-421/168/16	Omega Kancelarie Prawne Sp. Z o.o., Warszawa, ul. Poznańska 3/18 oraz Siedlce, ul. Kilińskiego 7/4	z urzędu	usunięto uchybienia
119.	19.28.10.2016 zmiana 24-28.10 i 02-03 11. oraz 07.10.11.2016 DIS-K-421/169/16	Komenda Główna Policji, Warszawa, ul. Puławska 148/150	z urzędu	
120.	24-28.10.2016 DIS-K-421/170/16	Adam Pietrak Komornik Sądowy przy Sądzie Rejonowym w Łodzi – Kancelaria Komornicza, al. Kościuszki 106/116	z urzędu	Zakończona – pismo inf. A. Pietraka o rezygnacji pełnienia obowiązków komornika sądowego
121.	24-28.10.2016 zmiana 24-27.10.2016 DIS-K-421/171/16	Liberty Poland S.A., Chorzów, ul. Katowicka 47	z urzędu	materiał dowodowy zostanie w całości wykorzystany do DIS-K-421/137/16
122.	24-28.10.2016 DIS-K-421/172/16	Lycamobile Sp. Z o.o., Warszawa, ul. Rzymowskiego 34/R34	Departament Orzecznictwa Legislacji i Skarg	decyzja GIODO
123.	25-28.10.2016 DIS-K-421/173/16	Ministerstwo Środowiska, Warszawa, ul. Wawelska 52/54	W związku z DIS-K-421/105/16	wszczęcie postępowania administracyjnego
124.	24-28.10.2016 DIS-K-421/174/16	PELAGROS Sp. Z o.o., Warszawa, al. Prymasa Tysiąclecia 46	z urzędu	decyzja GIODO
125.	08-10.11.2016 zmiana 07-08.11.2016 DIS-K-421/176/16	Anna Janczewska-Domagała prowadząca dział. gosp. Pod firmą 1) SHT Anna Janczewska-Domagała 2) Mobile Training s.c. Gabinet Medycyny Estetycznej Dr Sławomir	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg

		Koryśko, Warszawa, ul. Żytnia 18 lok. G		
126.	14-16.11.2016 DIS-K-421/177/16	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
127.	14-18.11.2016 zmiana 14-16.11.2016 DIS-K-421/178/16	Kancelaria Radcy Prawnego „PRELEX” Katarzyna Pawlonka-Jurczyk, Warszawa, ul. Josepha Conrada 18/284	z urzędu	nie stwierdzono uchybień
128.	14.18.11.2016 DIS-K-421/179/16	Primeon Sp. Zo.o., Warszawa, ul. Słowicza 43	z urzędu	
129.	16-18 i 21-22.11.2016 zmiana 16-18 i 21.11.2016 DIS-K-421/180/16	Kancelaria Warszawscy Adwokaci Twarowska-Handzlik & Biedka Sp. j., Warszawa, ul. Łucka 18/61	z urzędu	decyzja GIODO
130.	21-25.11.2016 zmiana 21-24.11.2016 DIS-K-421/181/16	Kancelaria Adwokacka Jolanty Mrówczyńskiej, Włocławek, Plac Wolności 17	z urzędu	nie stwierdzono uchybień
131.	21-25.11.2016 DIS-K-421/182/16	Yabimo Sp. Z o.o. Services Sp. k., Tarnów ul. St. Konarskiego 9	z urzędu	wszczęcie postępowania administracyjnego
132.	21-25.11.2016 zmiana 21-24.11.2016 DIS-K-421/183/16	TELECARE S.A., Zawiercie, ul. Samuela Huldczyńskiego 16 A	Departament Rejestracji	usunięto uchybienia
133.	28.11. – 02.12.2016 zmiana 29-30.11.2016 DIS-K-421/184/16	Kancelaria Radcy Prawnego Tomasz Okoniewski, Lublin, ul. Racławicka 8/23	z urzędu	usunięto uchybienia

134.	28.11.- 02.12.2016 zmiana 28-29.11.2016 DIS-K-421/185/16	Kancelaria Radcy Prawnego Radosław Ciesielski, Lublin, ul. Racławicka 8/23	z urzędu	usunięto uchybienia
135.	28.11.- 02.12.2016 zmiana 28-29.11.2016 DIS-K-421/186/16	Kancelaria Radcy Prawnego Marek Gołąb, Lublin, ul. Racławicka 8/23	z urzędu	usunięto uchybienia
136.	28.11. – 02.12.2016 DIS-K-421/187/16	Dariusz Karasiński Komornik Sądowy przy Sądzie Rejonowym w Środzie Wielkopolskiej – Kancelaria Komornicza, Środa Wielkopolska, oś. Piastowskie 38	z urzędu	wszczęcie postępowania administracyjnego
137.	28.11. – 02.12.2016 DIS-K-421/188/16	Komenda Powiatowa Policji w Brzesku, Brzesk, ul. Szczepanowska 53	z urzędu	nie stwierdzono uchybień
138.	30.11. -02.12.2016 DIS-K-421/189/16	Powszechna Kasa Oszczędności Bank Polski S.A., Warszawa, ul. Puławska 15	z urzędu	materiał dowodowy przekazano do sprawy DIS-K-421/31/16
139.	05-09.12.2016 zmiana 05-08.12.2016 DIS-K-421/190/16	Wolter Kluwer S.A., Warszawa, ul. Przyokopowa 33	z urzędu	nie stwierdzono uchybień
140.	05-09.12.2016 DIS-K-421/191/16	Mazowiecki Szpital Bródnowski w Warszawie Sp. z o.o., Warszawa, ul. Kondratowicza 8	Departament Orzecznictwa Legislacji i Skarg	nie stwierdzono uchybień
141.	05.09.12.2016 DIS-K-421/192/16	NOVO Technologies S.A., warszawa, ul. Cybernetyki 7B	z urzędu	usunięto uchybienia

142.	06-09.12.2016 DIS-K-421/193/16	Komenda Wojewódzka Policji w Krakowie, Kraków, ul. Mogilska 109	z urzędu	nie stwierdzono uchybień
143.	06-09.12.2016 DIS-K-421/194/16	American School of Warsaw, Bielawa, ul. Warszawska 202	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
144.	12-16.12.2016 DIS-K-421/195/16	Kancelaria Radców Prawnych Kozłowski, Pisarkiewicz-Firek Sp. j., Kraków, ul. Grodzka 60	z urzędu	usunięto uchybienia
145.	12-16.12.2016 DIS-K-421/196/16	Piotr Pietrasik, Komornik Sądowy przy Sądzie Rejonowym dla Łodzi – Widzewa w Łodzi – Kancelaria Komornicza, Łódź, ul. Kolumny 155	z urzędu	wszczęcie postępowania administracyjnego
146.	12-16.12.2016 DIS-K-421/197/16	Wspólnota Mieszkaniowa Krzywoustego 19 E, Gdańsk, ul. Krzywoustego 19E/7	Departament Orzecznictwa Legislacji i Skarg	wnioski przekazano do Departamentu Orzecznictwa Legislacji i Skarg
147.	19-23.12.2016 DIS-K-421/199/16	Kamil Pietrasik, Komornik Sądowy przy Sądzie Rejonowym dla Łodzi – Widzewa w Łodzi – Kancelaria Komornicza	z urzędu	wszczęcie postępowania administracyjnego

Załącznik nr 3

Załącznik nr 6 Wykaz podmiotów, do których zostało w 2016 r. skierowane wystąpienie o dokonanie sprawdzenia.

Lp.	Data i sygnatura wystąpienia	Podmiot, do którego skierowano wystąpienie o dokonanie sprawdzenia	Rozstrzygnięcie
1	08.03.2016 r., DIS-K-421/34/16/SPR 1	BPI Bank Polskich Inwestycji S.A., Warszawa ul. Przyokopowa 33	nie stwierdzono uchybień
2.	08.03.2016 r., DIS-K-421/35/16/SPR 2	Idea Bank S.A. Warszawa ul. Przyokopowa 33.	usunięto uchybienia
3.	08.03.2016 r., DIS-K-421/36/16/SPR 3	Ikano Bank AB (publ) Spółka Akcyjna Oddział w Polsce, Warszawa, ul. Postępu 21B.	decyzja GIODO
4.	08.03.2016 r., DIS-K-421/37/16/SPR 4	Getin Noble Bank S.A. Warszawa, ul. Przyokopowa 33.	nie stwierdzono uchybień
5.	08.03.2016 r., DIS-K-421/38/16/SPR 5	PKO Bank Hipoteczny S.A., Gdynia, Pl. Kaszubski 17/19/21	nie stwierdzono uchybień
6.	08.03.2016 r., DIS-K-421/39/16/SPR 6	mBank Hipoteczny S.A., Warszawa, Al. Armii Ludowej 26. D	nie stwierdzono uchybień
7.	15.03.2016 r., DIS-K-421/42/16/SPR 7	PLUS BANK S.A., Warszawa Al. Stanów Zjednoczonych 61A.	decyzja GIODO
8.	15.03.2016 r., DIS-K-421/43/16/SPR 8	Santander Consumer Bank S.A., Wrocław ul. Strzegomska 42C	decyzja GIODO

9.	15.03.2016 r., DIS-K-421/44/16/SPR 9	Bank Pocztowy S.A., Bydgoszcz ul. Jagiellońska 17	decyzja GIODO
10.	15.03.2016 r., DIS-K-421/45/16/SPR 10	Toyota Bank Polska S.A., Warszawa, ul Postępu 18B	decyzja GIODO
11.	15.03.2016 r., DIS-K-421/46/16/SPR 11	Deutsche Bank Polska S.A., Warszawa, Al. Armii Ludowej 26	
12.	18.04.2016 r., DIS-K-421/62/16/SPR12	Bank Spółdzielczy w Sandomierzu, Sandomierz, ul. Słowackiego 37b	nie przetwarza danych w badanym zakresie
13.	18.04.2016 r., DIS-K-421/63/16/SPR13	Bank Spółdzielczy w Świdnicy, Świdnica, ul. Długa 9	nie stwierdzono uchybień
14.	18.04.2016 r., DIS-K-421/64/16/SPR14	Bank Spółdzielczy w Kielcach, Kielce, ul. Złota 9	decyzja GIODO
15.	18.04.2016 r., DIS-K-421/65/16/SPR15	Bank Spółdzielczy w Gnieźnie, Gniezno, ul. Dąbrówki 19	decyzja GIODO
16.	25.04.2016 r., DIS-K-421/70/16/SPR16	Bank Spółdzielczy w Gostyninie, Gostynin, ul. Rynek 4/5	usunięto uchybienia
17.	25.04.2016 r., DIS-K-421/71/16/SPR17	Bank Spółdzielczy w Tczewie, Tczew, ul. Ignacego Paderewskiego 1	nie przetwarza danych w badanym zakresie
18.	25.04.2016 r., DIS-K-421/72/16/SPR18	Bank Spółdzielczy w Santoku, Santok, ul. Gralewska 6 B	decyzja GIODO

19.	26.04.2016 r., DIS-K-421/73/16/SPR19	Bank Spółdzielczy w Dębicy, Dębica, ul. Rzeszowska 14	nie przetwarza danych w badanym zakresie
20.	26.04.2016 r., DIS-K-421/74/16/SPR20	Bank Spółdzielczy w Augustowie, Augustów, ul. 3 Maja 13	nie przetwarza danych w badanym zakresie
21.	30.08.2016 r., DIS-K-421/125/16/SPR 21	Towarzystwo Ubezpieczeń na Życie Warta S.A., Warszawa, ul. Chmielna 85/87	
22.	30.08.2016 r., DIS-K-421/126/16/SPR 22	Uniqa Towarzystwo Ubezpieczeń na Życie S.A., Łódź, ul. Gdańska 132	
23.	30.08.2016 r., DIS-K-421/127/16/SPR 23	Vienna Life Towarzystwo Ubezpieczeń na Życie S.A. Vienna Insurance Group, Warszawa, ul. Cybernetyki 7 (Do 20.10.2116 Skandia Życie Towarzystwo Ubezpieczeń S.A.)	
24.	30.08.2016 r., DIS-K-421/128/16/SPR 24	Polisa Życie Towarzystwo Ubezpieczeń S.A. Vienna Insurace Group, Warszawa, al. Jerozolimskie 162A	
25.	30.08.2016 r., DIS-K-421/12916/SPR 25	Pocztowe Towarzystwo Ubezpieczeń na Życie S.A., Warszawa, ul Domaniewska 50A	
26.	31.08.2016 r., DIS-K-421/130/16/SPR 26	Towarzystwo Ubezpieczeń Inter – Życie Polska S.A., Warszawa, al. Jerozolimskie 172	
27.	31.08.2016 r., DIS-K-421/131/16/SPR 27	Signal Iduna Życie Polska Towarzystwo Ubezpieczeń S.A., Warszawa, ul. Przyokopowa 31	
28.	31.08.2016 r., DIS-K-421/132/16/SPR 28	Generali Życie Towarzystwo Ubezpieczeń S.A., Warszawa, ul. Postępu 15 B	

29.	31.08.2016 r., DIS-K-421/133/16/SPR 29	Towarzystwo Ubezpieczeń na Życie Europa S.A., Wrocław ul. Gwiaździsta 62	
30.	31.08.2016 r., DIS-K-421/134/16/SPR 30	Sopockie Towarzystwo Ubezpieczeń na Życie ERGO Hestia S.A., Sopot, ul. Hestii 1	
31.	21.09.2016 r. DIS-K-421/145/16/SPR 31	Urząd Gminy Hrubieszów, Hrubieszów, ul. B. Prusa 8	nie stwierdzono uchybień
32.	21.09.2016 r. DIS-K-421/146/16/SPR 32	Urząd Miasta Bielsko – Biała, Bielsko - Biała, Pl. Ratuszowy 1	nie stwierdzono uchybień
33.	21.09.2016 r. DIS-K-421/147/16/SPR 33	Urząd Gminy Wolsztyn, Wolsztyn, ul. Rynek 1	nie stwierdzono uchybień
34.	21.09.2016 r. DIS-K-421/148/16/SPR 34	Urząd Miasta Dzierżoniów, Dzierżoniów, ul. Rynek 1	nie stwierdzono uchybień
35.	21.09.2016 r. DIS-K-421/149/16/SPR 35	Urząd Gminy Kwidzyn, Kwidzyn, ul. Grudziądzka 30	nie stwierdzono uchybień
36.	05.10.2016 r., DIS-K-421/156/16/SPR 36	Urząd Gminy Cedynia, Cedynia, Pl. Wolności 1	decyzja GIODO
37.	05.10.2016 r., DIS-K-421/157/16/SPR 37	Urząd Gminy Krobia, Krobia, ul. Rynek 1	nie stwierdzono uchybień
38.	05.10.2016 r., DIS-K-421/158/16/SPR 38	Urząd Gminy Rzeczenica, Rzeczenica, ul. Człuchowska 26	nie stwierdzono uchybień
39.	05.10.2016 r.,	Urząd Miasta Stalowa Wola, Stalowa Wola, ul. Wolności 7	

	DIS-K-421/159/16/SPR 39		nie stwierdzono uchybień
40.	05.10.2016 r., DIS-K-421/160/16/SPR 40	Urząd Gminy Nowa Ruda, Nowa Ruda, ul. Niepodległości 1	nie stwierdzono uchybień
41.	06.10.2016 r., DIS-K-421/161/16/SPR 41	Urząd Gminy Węgorzewo, Węgorzewo, ul. Zamkowa 3	nie stwierdzono uchybień
42.	06.10.2016 r., DIS-K-421/162/16/SPR 42	Urząd Miasta Wisła, Wisła, Pl. Bogumiła Hoffa 3	decyzja GIODO
43.	06.10.2016 r., DIS-K-421/163/16/SPR 43	Urząd Gminy Bolków, Bolków, ul. Rynek 1	decyzja GIODO
44.	06.10.2016 r., DIS-K-421/164/16/SPR 44	Urząd Gminy Kleszczów, Kleszczów, ul. Główna 47	nie stwierdzono uchybień
45.	06.10.2016 r., DIS-K-421/165/16/SPR 45	Urząd Gminy Sztutowo, Sztutowo, ul. Gdańska 55	nie stwierdzono uchybień

Załącznik nr 4

Wykaz orzeczeń wydanych w 2016 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	Sygnatura decyzji/sprawy	Przedmiot sprawy	Rozstrzygnięcie
1	2016-01-07 II SA/Wa 1238/15	DOLiS/DEC-446/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych nakazującą usunięcie danych osobowych w pozostałym zakresie odmawiającą uwzględnienia wniosku	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
2	2016-01-08 II SA/Wa 657/15	DOLiS/DEC-109/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
3	2016-01-12 II SA/Wa 1217/15	DOLiS/DEC-260/14	Skarga na decyzję w przedmiocie przetwarzania danych osobowych nakazującą udostępnienie danych osobowych	Wyrok WSA - Oddalono skargę
4	2016-01-12 II SA/Wa 659/15	DOLiS/DEC-188/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
5	2016-01-14 II SAB/Wa 820/15	DOLiS-440-1640/14	Skarga na bezczynność organu	Wyrok WSA - Oddalono skargę
6	2016-01-14 II SAB/Wa 1125/15	DOLiS-440-793/15	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę

7	2016-01-15 I OSK 1681/15	DOLiS-440-1126/12	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 12 lutego 2015 r. (II SAB/Wa 586/14) w sprawie ze skargi na przewlekłość GIODO w przedmiocie prowadzenia postępowania w sprawie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
8	2016-01-19 II SA/Wa 533/15	DOLiS/DEC-58/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych utrzymującą w mocy decyzję umarzającą postępowanie	Wyrok WSA - Oddalono skargę
9	2016-01-19 I OSK 3485/15	DOLiS/DEC-1/15	Skarga kasacyjna na postanowienie WSA w Warszawie z dnia 7 lipca 2015 r. (II SA/Wa 449/15) o odrzuceniu skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Oddalono skargę kasacyjną
10	2016-01-20 II SA/Wa 1190/15	DOLiS/DEC-413/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych odmawiającą uwzględnienia wniosku	Wyrok WSA - Oddalono skargę
11	2016-01-21 II SAB/Wa 867/15	DOLiS-440-485/15	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Oddalono skargę
12	2016-01-22 II SA/Wa 830/15	DOLiS/POST-83/15	Skarga na postanowienie w przedmiocie odmowy wydania stronie postępowania kopii akt	Wyrok WSA - Oddalono skargę
13	2016-01-25 II SA/Wa 2062/15	DOLiS/DEC-804/15	Skarga na decyzję w przedmiocie uaktualnienia danych osobowych	Postanowienie WSA - Wstrzymano wykonanie zaskarżonej decyzji
14	2016-01-25 II SAB/Wa 1/16	DOLiS-440-895/12	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę

15	2016-01-26 II SA/Wa 943/15	DOLiS/DEC-1086/14	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
16	2016-01-26 II SAB/Wa 1041/15	DOLiS-440-433/14	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Zobowiązano do wydania decyzji i stwierdzono, że przewlekłe prowadzenie postępowania miało miejsce z rażącym naruszeniem prawa
17	2016-01-26 II SA/Wa 1301/15	DOLiS/DEC-478/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
18	2016-01-26 II SAB/Wa 1085/15	DOLiS-440-349/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność miała miejsce z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie
19	2016-01-27 II SA/Wa 1026/15	DOLiS/DEC-326/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych nakazującą wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych poprzez usunięcie danych osobowych we wskazanym zakresie	Wyrok WSA - Oddalono skargę
20	2016-01-27 II SA/Wa 2049/15	DOLiS/DEC-845/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę

21	2016-01-27 II SA/Wa 1622/15	DOLiS/DEC- 592/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
22	2016-01-28 II SA/Wa 2107/15	DOLiS/DEC- 822/15	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Postanowienie WSA - Wstrzymano wykona- nie zaskarżonej decy- zji
23	2016-01-28 II SAB/Wa 1095/15	DOLiS-440- 876/15	Skarga na bezczynność organu	Postanowienie WSA - Umorzono postępowa- nie z art. 161 ustawy p.p.s.a.
24	42397 II SA/Wa 1939/15	DOLiS/DEC- 117/15	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA - Odrzucono skargę
25	2016-01-28 II SA/Wa 1218/15	DOLiS/DEC- 454/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
26	2016-01-29 II SA/Wa 1088/15	DOLiS/DEC- 364/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
27	2016-02-01 II SA/Wa 1336/15	DIS/DEC- 964/467/15/45251	Zapewnienie osobom składającym wniosek o wydanie Poznańskiej Elektronicznej Karty Aglo- meracyjnej (Karta PEKA) możliwości wyrażenia swobodnego oświadcze- nia woli, którego treścią jest zgoda na przetwarza- nie danych osobowych tj. Wyodrębnienie zgody na przetwarzanie danych osobowych w celach	oddalenie skargi

			marketingowych od zgody na otrzymywanie informacji marketingowych i handlowych za pomocą środków komunikacji elektronicznej.	
28	2016-02-03 II SA/Wa 2032/15	DOLiS/DEC-790/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
29	2016-02-09 I OSK 579/15	DOLiS/DEC-171/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 19 listopada 2014 r. (II SA/Wa 727/14) uchylającego zaskarżoną decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
30	42409 I OSK 3179/15	DOLiS/DEC-932/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 9 lipca 2015 r. (II SA/Wa 2095/14) uchylającego zaskarżoną decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
31	42409 I OSK 1466/15	DOLiS/DEC-186/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 14 stycznia 2015 r. (II SA/Wa 791/14) uchylającego zaskarżoną decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną

32	2016-02-09 I OSK 1509/15	DOLiS/DEC-419/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 16 lutego 2015 r. (II SA/Wa 1242/14) uchylającego zaskarżoną decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
33	2016-02-09 I OSK 2691/15	DOLiS/DEC-639/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 29 kwietnia 2015 r. (II SA/Wa 1604/14) uchylającego zaskarżoną decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
34	2016-02-09 I OSK 2585/15	DOLiS/DEC-228/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 22 kwietnia 2015 r. (II SA/Wa 847/14) uchylającego zaskarżoną decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
35	2016-02-12 I OZ 96/16	DOLiS/DEC-545/15	Zażalenie na postanowienie WSA w Warszawie z dnia 7 grudnia 2015 r. (II SA/Wa 1353/15) o wstrzymaniu wykonania decyzji w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobowych	Postanowienie NSA - Oddalono zażalenie
36	2016-02-15 II SA/Wa 1489/15	DOLiS/DEC-569/15	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA - Odrzucono skargę

37	2016-02-17 II SA/Wa 113/16	DOLiS/DEC-877/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odmówiono wstrzymania wykonania zaskarżonej decyzji
38	2016-02-17 II SAB/Wa 1160/15	DOLiS-440-942/15	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
39	2016-02-17 II SA/Wa 894/15	DOLiS/DEC-288/15	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Wyrok WSA - Oddalono skargę
40	2016-02-18 II SA/Wa 1409/15	DOLiS/DEC-552/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
41	2016-02-18 II SA/Wa 1655/15	DIS/DEC-622/15/67982	Sformułowanie zgody na przetwarzanie przez spółkę danych transmisyjnych dla celów marketingu usług spółki w sposób odrębny od zgody dla celu marketingu usług podmiotów, z którymi spółka współpracuje. Zapewnienie osobom fizycznym zawierającym ze spółką umowę o świadczenie usług telekomunikacyjnych – za pośrednictwem internetowego oraz telefonicznego kanału sprzedaży – swobody w kwestii wyrażenia zgody na przetwarzanie danych osobowych widniejących w dowodzie osobistym, a wykraczających poza art. 161 ust. 2 Ustawy Prawo telekomunikacyjne.	oddalenie skargi

42	2016-02-19 I OSK 3111/14	DOLiS/DEC-5/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 21 sierpnia 2014 r. (II SA/Wa 389/14) uchylającego zaskarżoną decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
43	2016-02-22 II SA/Wa 895/15	DOLiS/DEC-293/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych odmawiającą nakazania udostępnienia danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
44	2016-02-22 II SA/Wa 1654/15	DOLiS/DEC-716/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
45	2016-02-23 II SAB/Wa 1161/15	DOLiS-440-94/13	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA - Odrzucono skargę
46	2016-02-26 II SA/Wa 124/16	DOLiS/DEC-894/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odmówiono wstrzymania wykonania zaskarżonej decyzji
47	2016-03-01 II SA/Wa 1333/15	DOLiS/DEC-511/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
48	2016-03-02 II SA/Wa 1488/15	DOLiS/DEC-580/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
49	2016-03-02 II SA/Wa 1353/15	DOLiS/DEC-545/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję

			uaktualnienie danych osobowych	
50	2016-03-02 II SAB/Wa 1134/15	DOLiS-440-2089/14	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
51	2016-03-03 II SA/Wa 1174/15	DOLiS/DEC-407/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
52	2016-03-04 II SA/Wa 1289/15	DOLiS/DEC-434/15	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję
53	2016-03-07 II SAB/Wa 88/16	DOLiS-440-661/15	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA - Odrzucono skargę
54	2016-03-08 II SA/Wa 1487/15	DOLiS/DEC-568/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych nakazującą udostępnienie danych osobowych	Wyrok WSA - Oddalono skargę
55	2016-03-08 II SA/Wa 1451/15	DOLiS/DEC-572/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
56	2016-03-09 II SAB/Wa 891/15	DOLiS-440-400/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność nie miała miejsca z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie
57	2016-03-09 II SAB/Wa 890/15	DOLiS-440-285/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność nie miała miejsca z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie

58	2016-03-09 II SAB/Wa 958/15	DOLiS-440-1683/14	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono, iż przewlekłe prowadzenie postępowania nie miało miejsca z rażącym naruszeniem prawa
59	2016-03-09 I OZ 208/16	DOLiS-440-895/12	Zażalenie na postanowienie WSA w Warszawie z dnia 25 stycznia 2016 r. (II SAB/Wa 1/16) w sprawie ze skargi na bezczynność GIODO po wyroku WSA w Warszawie z dnia 29 stycznia 2014 r. (II SA/Wa 1819/13)	Postanowienie NSA - Uchylono zaskarżone postanowienie
60	2016-03-11 II SA/Wa 1303/15	DOLiS/DEC-504/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
61	2016-03-11 II SA/Wa 1302/15	DOLiS/DEC-512/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
62	2016-03-14 II SA/Wa 1754/15	DOLiS/DEC-702/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
63	2016-03-14 II SA/Wa 265/16	DOLiS/DEC-588/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odmówiono przywrócenia terminu do wniesienia skargi
64	2016-03-14 II SA/Wa 44/16	DIS/POST-475/15/94665 DIS-K-421/125/15	Skarga na postanowienie GIODO o kontynuowaniu kontroli.	odrzucenie skargi

65	2016-03-16 II SA/Wa 1645/15	DOLiS/DEC- 694/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
66	2016-03-17 II SA/Wa 2014/15	DOLiS/DEC- 792/16	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
67	2016-03-17 II SA/Wa 2062/15	DOLiS/DEC- 804/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
68	2016-03-18 II SA/Wa 2033/15	DOLiS/DEC- 803/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
69	2016-03-18 II SA/Wa 1940/15	DOLiS-440-72/14	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
70	2016-03-22 II SA/Wa 1800/15	DOLiS/DEC- 680/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
71	2016-03-22 II SAB/Wa 956/15	DOLiS-440- 1059/13	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
72	2016-03-22 II SAB/Wa 876/15	DOLiS-440- 988/12	Skarga na bezczynność organu	Wyrok WSA - Stwier- dzono, iż bezczynność miała miejsce z rażą- cym naruszeniem

				prawa i w pozostałym zakresie umorzono postępowanie
73	2016-04-05 II SA/Wa 69/16	DOLiS/DEC-564/13	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - Oddalono skargę
74	2016-04-13 II SA/Wa 392/16	DOLiS/DEC-985/15	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA - Wstrzymano wykonanie zaskarżonej decyzji
75	2016-04-13 II SA/Wa 1653/15	DOLiS/DEC-700/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
76	2016-04-13 I OSK 1065/15	DOLiS/DEC-173/14	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 27 listopada 2014 r. (II SA/Wa 792/14) w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
77	2016-04-13 II SA/Wa 2208/15	DOLiS/POST-457/15	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku o kopię akt	Postanowienie WSA - Odrzucono skargę
78	2016-04-13 II SAB/Wa 140/16	DOLiS-440-1059/13	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
79	2016-04-13 I OSK 1569/15	DOLiS/DEC-264/14	Skarga kasacyjna GIODO i strony postępowania od wyroku WSA w Warszawie z dnia 13 listopada 2014 r. (II SA/Wa 875/14) w sprawie ze skargi na decyzję w przedmiocie odmowy stwierdzenia nieprawidłowości w przetwarzaniu i udostępnianiu danych osobowych.	Wyrok NSA - Oddalono skargi kasacyjne

80	2016-04-13 I OSK 629/15	DIS/DEC-276/14/22915	Usunięcie uchybień poprzez: Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych przesyłanych za pomocą formularza kontaktowego ujawnij. pl. Opracowanie i wdrożenie dokumentacji przetwarzania danych. Wyznaczenie administratora bezpieczeństwa informacji. Nadanie osobom dopuszczonym do przetwarzania danych upoważnień do przetwarzania danych osobowych. Opracowanie ewidencji osób upoważnionych do przetwarzania danych. Określenie w umowie zawartej z Grupa Gram Sp.z o.o. Zakresu i celu powierzenia przetwarzania danych osobowych przetwarzanych w ramach portalu ujawnij.pl	Uchylenie zaskarżonego wyroku i przekazanie do WSA do ponownego rozpatrzenia.
81	2016-04-15 II SA/Wa 265/16	DOLiS/DEC-588/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych postanawia	Postanowienie WSA - Odrzucono skargę
82	2016-04-15 II SA/Wa 1335/15	DOLiS/DEC-584/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
83	2016-04-15 II SAB/Wa 1149/15	DOLiS-440-752/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdza, że GIODO dopuścił się bezczynności

				w rozpatrzeniu sprawy, jednakże bezczynność ta nie miała miejsca z rażącym naruszeniem prawa
84	2016-04-18 II SAB/Wa 990/15	DOLiS-440-1540/13	Skarga na bezczynność organu	Wyrok WSA - Stwierdza, że GIODO dopuścił się bezczynności i stwierdza, że bezczynność organu miała miejsce z rażącym naruszeniem prawa
85	2016-04-18 II SAB/Wa 1071/15	DOLiS-440-573/13	Skarga na bezczynność organu	Wyrok WSA - Stwierdza, że GIODO dopuścił się bezczynności i stwierdza, że bezczynność organu miała miejsce z rażącym naruszeniem prawa
86	2016-04-21 II SA/Wa 461/16	DOLiS/DEC-12/16	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA - Odmówiono wstrzymania wykonania zaskarżonej decyzji oraz decyzji ją poprzedzającej
87	2016-04-21 I OSK 2245/14	DOLiS/POST-274/13	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 20 maja 2014 r. (II SA/Wa 2013/13) w sprawie ze skargi na postanowienie w przedmiocie zwrotu skargi	Wyrok NSA - Oddalono skargę kasacyjną
88	2016-04-21 I OZ 346/16	DOLiS/DEC-877/15	Zażalenie na postanowienie WSA w Warszawie z dnia 17 lutego 2016 r. (II SA/Wa 113/16) o odmowie wstrzymania wykonania zaskarżonej decyzji w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Uchylono zaskarżone postanowienie i wstrzymano wykonanie zaskarżonej decyzji

89	2016-04-26 II SA/Wa 1740/15	DOLiS/DEC- 721/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję
90	2016-04-26 II SAB/Wa 226/16	DOLiS-440- 474/13	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
91	2016-04-26 II SAB/Wa 165/16	DOLiS-440- 1281/14	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
92	2016-04-28 II SA/Wa 2081/15	DOLiS/DEC- 797/15	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
93	2016-04-28 VIII SA/Wa 185/16	DOLiS/DEC- 978/15	Skarga na decyzję w przedmiocie uaktual- nienia danych osobowych	Postanowienie WSA - Umorzono postępowa- nie z art. 161 ustawy p.p.s.a.
94	2016-04-29 I OSK 252/15	DOLiS/DEC- 983/13	Skarga kasacyjna od wy- roku WSA w Warszawie z dnia 24 września 2014 r. (II SA/Wa 2200/13) w sprawie ze skargi na decyzję w przedmiocie ochrony danych osobo- wych	Wyrok NSA - Odda- lono skargę kasacyjną
95	2016-05-06 II SAB/Wa 97/16	DOLiS-440- 1188/13	Skarga na przewlekłe prowadzenie postępowa- nia	Wyrok WSA - Orze- czono o wymierzeniu grzywny za przewlekłe prowadzenie postępo- wania przez organy - art. 149 § 2 p.p.s.a.
96	2016-05-09 II SA/Wa 378/16	DOLiS/DEC- 974/15	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Postanowienie WSA - Odrzucono skargę
97	2016-05-12 II SAB/Wa 181/16	DOLiS-440- 1212/14	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę

98	2016-05-12 II SA/Wa 1713/15	DOLiS/DEC- 660/15	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Wyrok WSA - Odda- lono skargę
99	2016-05-12 II SA/Wa 2107/15	DOLiS/DEC- 822/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję
100	42502 II SA/Wa 299/16	DOLiS/DEC-46/16	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgod- nego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
101	2016-05-12 II SO/Wa 16/16	GI-DS-430/614/02	Wniosek o wymierzenie GIODO grzywny za nie- przekazanie odpowiedzi na skargę i akt w spra- wie II SAB/Wa 1129/15	Postanowienie WSA - Oddalono wniosek o wymierzenie grzywny art. 55 ustawy p.p.s.a.
102	2016-05-16 II SAB/Wa 176/16	DOLiS-440- 1383/14	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
103	2016-05-16 II SA/Wa 533/16	DOLiS/DEC-58/16	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych postanawia	Postanowienie WSA - Odrzucono skargę
104	2016-05-17 II SAB/Wa 1099/15	DOLiS-440- 785/13	Skarga na przewlekłe prowadzenie postępowa- nia	Wyrok WSA - Stwier- dzono, iż przewlekłe prowadzenie postępo- wania miało miejsca z rażącym narusze- niem prawa i wymie- rzono organowi grzywnę
105	2016-05-18 II SA/Wa 1941/15	DOLiS/DEC- 779/15	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję
106	2016-05-18 II SAB/Wa 1120/15	DOLiS-440- 2481/14	Skarga na przewlekłe prowadzenie postępowa- nia	Wyrok WSA - Stwier- dzono przewlekłość

				postępowania administracyjnego i że przewlekłość postępowania miała charakter rażący
107	2016-05-18 I OSK 579/15	DOLiS/DEC-171/14	Wniosek o uzupełnienie wyroku NSA z dnia 9 lutego 2016 r. (I OSK 579/15) oddalającego skargę kasacyjną GIODO	Postanowienie NSA - Uzupełniono wyrok
108	2016-05-19 II SAB/Wa 1116/15	DOLiS-440-2382/14	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność miała miejsce z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie
109	2016-05-19 II SA/Wa 126/16	DOLiS/DEC-909/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
110	2016-05-20 II SA/Wa 1652/15	DOLiS/DEC-655/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
111	2016-05-20 II SA/Wa 446/16	DOLiS/DEC-885/15	Skarga na decyzję w przedmiocie odmowy uwzględnienia wniosku w sprawie skargi na przetwarzanie danych osobowych	Postanowienie WSA - Odrzucono skargę
112	2016-05-20 II SA/Wa 1781/15	DOLiS/DEC-689/15	Skarga na decyzję w przedmiocie nakazu przywrócenia stanu zgodnego z prawem poprzez uaktualnienie danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
113	2016-05-23 II SAB/Wa 251/16	DOLiS-440-876/15	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę

114	2016-05-24 II SA/Wa 570/16	DOLiS/DEC-13/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
115	2016-05-24 I OSK 508/16	DOLiS/DEC-9/15	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 24 listopada 2015 r. (II SA/Wa 324/15) w sprawie ze skargi na decyzję w przedmiocie uaktualnienia danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
116	2016-05-24 I OSK 453/16	DOLiS/DEC-58/15	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 2 grudnia 2015 r. (II SA/Wa 545/15) w sprawie ze skarg na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
117	2016-05-24 I OSK 411/16	DOLiS/DEC-427/1	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 24 listopada 2015 r. (II SA/Wa 1154/15) w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
118	2016-05-24 I OSK 276/16	DOLiS/DEC-1101/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 19 października 2015 r. (II SA/Wa 86/15) w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
119	2016-05-24 I OSK 277/16	DOLiS/POST-25/16	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 28 października 2015 r. (II	Postanowienie NSA - Umorzono postępowanie przed Naczelnym

			SA/Wa 486/15) w sprawie ze skargi na postanowienie w przedmiocie odmowy uwzględnienia wniosku o wyjaśnienie wątpliwości co do treści decyzji	Sądem Administracyjnym
120	2016-05-24 I OSK 275/16	DOLiS/DEC-289/15	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 12 listopada 2015 r. (II SA/Wa 942/15) w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
121	2016-05-24 I OSK 238/16	DOLiS/DEC-1129/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 28 października 2015 r. (II SA/Wa 183/15) w sprawie ze skargi na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
122	2016-05-24 I OSK 3434/15	DOLiS/DEC-882/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 2 września 2015 r. (II SA/Wa 1881/14) w sprawie ze skargi na uzasadnienie decyzji oraz sprawy ze skargi na decyzję Generalnego Inspektora Ochrony Danych Osobowych w przedmiocie uaktualnienia danych osobowych	Postanowienie NSA - Umorzono postępowanie przed Naczelnym Sądem Administracyjnym
123	2016-05-24 II SA/Wa 2172/15	DOLiS/POST-469/15	Skarga na postanowienie w przedmiocie zwrotu pisma	Wyrok WSA - Oddalono skargę

124	2016-05-27 II SA/Wa 1780/15	DOLiS/DEC-666/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych nakazującą zaprzestania przetwarzania danych	Wyrok WSA - Oddalono skargę
125	2016-05-27 II SA/Wa 528/16	DOLiS/DEC-60/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
126	2016-05-30 II SA/Wa 365/16	DOLiS/DEC-163/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
127	2016-05-30 II SA/Wa 347/16	DOLiS/DEC-980/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
128	42527 II SAB/Wa 287/16	DOLiS-440-848/15	Skarga na bezczynność organu	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
129	2016-06-07 II SAB/Wa 40/16	DOLiS-440-255/13	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono, iż przewlekłe prowadzenie postępowania miało miejsca z rażącym naruszeniem prawa
130	2016-06-07 II SAB/Wa 189/16	DOLiS-440-931/12	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność miała miejsca z rażącym naruszeniem prawa i wymierzono organowi grzywnę
131	2016-06-08 II SAB/Wa 1129/15	GI-DS-430/614/02	Skarga na bezczynność organu	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
132	2016-06-08 II SA/Wa 527/16	DOLiS/DEC-65/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z wniosku

				o wstrzymanie wykonania zaskarżonego aktu
133	2016-06-09 II SA/Wa 512/16	DOLiS/DEC-161/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
134	2016-06-10 II SAB/Wa 1062/15	DOLiS-440-895/12	Skarga na bezczynność organu	Wyrok WSA - Oddalono skargę
135	42531 II SAB/Wa 37/16	DOLiS-440-2270/14	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono, iż przewlekłe prowadzenie postępowania miało miejsca z rażącym naruszeniem prawa i wymierzono organowi grzywnę
136	2016-06-13 II SA/Wa 2018/15	DOLiS/DEC-771/15	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - Oddalono skargę
137	2016-06-16 II SA/Wa 654/16	DOLiS/DEC-118/16	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA - Odrzucono skargę
138	2016-06-16 II SAB/Wa 132/16	DOLiS-440-1133/15	Skarga na bezczynność organu	Wyrok WSA - Zobowiązano do rozpoznania skargi i stwierdzono, że bezczynność miała miejsce bez rażącego naruszenia prawa
139	2016-06-16 II SA/Wa 375/16	DOLiS/DEC-3/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
140	2016-06-21 II SA/Wa 463/16	DOLiS/DEC-11/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
141	2016-06-21 II SA/Wa 571/16	DOLiS/DEC-90/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.

142	2016-06-22 II SAB/Wa 86/16	DOLiS-440-951/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność miała miejsca z rażącym naruszeniem prawa
143	2016-06-23 II SAB/Wa 169/16	DOLiS-440-1668/14	Skarga na bezczynność organu	Wyrok WSA - Zobowiązano do rozpoznania skargi i stwierdzono, że bezczynność miała miejsce bez rażącego naruszenia prawa oraz orzeczono o wymierzeniu grzywny
144	2016-06-27 II SA/Wa 556/16	DOLiS/DEC-241/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
145	2016-06-28 II SA/Wa 2199/15	DOLiS/DEC-828/15	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Wyrok WSA - Oddalono skargę
146	2016-06-28 II SA/Wa 168/16	DOLiS/DEC-875/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
147	2016-06-28 II SA/Wa 32/16	DOLiS/DEC-864/15	Skarga na decyzję w przedmiocie umorzenia postępowania	Wyrok WSA - Oddalono skargę
148	2016-06-29 II SA/Wa 1825/15	DOLiS/DEC-678/15	Skarga na decyzję w przedmiocie uaktualnienia danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
149	2016-06-30 II SAB/Wa 1132/15	DOLiS-440-46/13	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność miała miejsce z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie
150	2016-07-06 II SAB/Wa 39/16	DOLiS-440-1563/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono, iż bezczynność nie miała miejsca z rażącym naruszeniem

				prawa i umorzono postępowanie w pozostałym zakresie
151	2016-07-06 II SAB/Wa 38/16	DOLiS-440-1360/15	Skarga na bezczynność organu	Wyrok WSA - Oddalono skargę
152	2016-07-06 I OSK 3086/15	DOLiS-440-1426/13	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 19 maja 2015 r. (II SAB/Wa 1002/14) w sprawie ze skargi na przewlekłość postępowania w przedmiocie rozpoznania skargi na przetwarzanie danych osobowych	Wyrok NSA - Oddalono skargę kasacyjną
153	2016-07-06 I OSK 3016/15	DOLiS-035-3972/14	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 25 czerwca 2015 r. (II SAB/Wa 305/15) w sprawie ze skargi na bezczynność w przedmiocie rozpatrzenia wniosku	Wyrok NSA - Uchylono zaskarżony wyrok i przekazano sprawę do ponownego rozpoznania przez Wojewódzki Sąd Administracyjny
154	2016-07-07 I OSK 1425/16	DOLiS-440-1640/14	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 14 stycznia 2016 r. (II SAB/Wa 820/15) w sprawie ze skargi na bezczynność w przedmiocie rozpoznania skargi	Wyrok NSA - Oddalono skargę kasacyjną
155	2016-07-14 II SA/Wa 2080/15	DOLiS/DEC-851/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
156	2016-07-20 II SA/Wa 1942/15	DOLiS/DEC-805/15	Skarga na decyzję w przedmiocie umorzenia postępowania	Postanowienie WSA - Odrzucono skargę
157	2016-07-20 II SA/Wa 225/16	DOLiS/POST-507/15	Skarga na postanowienie w przedmiocie odmowy wszczęcia postępowania	Wyrok WSA - Oddalono skargę

158	2016-07-20 II SAB/Wa 308/16	DOLiS-440-1599/15	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
159	2016-07-21 II SA/Wa 113/16	DOLiS/DEC-877/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
160	2016-07-26 II SAB/Wa 9/16	DOLiS-440-169/13	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Zobowiązano do zakończenia postępowania i stwierdzono, że przewlekłe prowadzenie postępowania miało miejsce z rażącym naruszeniem prawa oraz wymierzono grzywnę
161	26.07.2016r. II SA/Wa 460/16	DIS/DEC-4/16/684	Przetwarzanie bez podstawy prawnej danych adresatów przesyłek w zakresie adresów i informacji o zdarzeniach dotyczących nieodebrania/niedostarczania/zwrotu przesyłek.	ochylenie decyzji GIODO
162	2016-07-27 II SA/Wa 153/16	DOLiS/POST-509/15	Skarga na postanowienie w przedmiocie stwierdzenia niedopuszczalności	Wyrok WSA - Uchylono zaskarżone postanowienie
163	2016-07-28 II SA/Wa 461/16	DOLiS/DEC-12/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
164	2016-07-28 II SAB/Wa 222/16	DOLiS-440-1756/13	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono przewlekłe prowadzenie postępowania oraz, że bezczynność nie miała miejsca z rażącym naruszeniem prawa
165	2016-07-28 II SAB/Wa 162/16	DOLiS-440-895/12	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono, iż przewlekłe postępowania nie

				miało miejsca z rażącym naruszeniem prawa i w pozostałym zakresie umorzono postępowanie
166	2016-07-28 II SA/Wa 154/16	DOLiS/DEC-971/15	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - Oddalono skargę
167	2016-07-28 II SA/Wa 1363/15	DOLiS/DEC-491/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
168	2016-08-02 II SA/Wa 1111/16	DOLiS/DEC-332/16	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA - Odmówiono wstrzymania wykonania zaskarżonej decyzji
169	2016-08-03 II SAB/Wa 1162/15	DOLiS-440-996/15	Skarga na bezczynność organu	Wyrok WSA - Zobowiązano do rozpatrzenia wniosku w przedmiocie przetwarzania danych osobowych i stwierdzono, że bezczynność miała miejsce z rażącym naruszeniem prawa oraz wymierzono organowi grzywnę
170	2016-08-05 II SA/Wa 2147/15	DOLiS/DEC-833/15	Skarga na decyzję w przedmiocie ochrony danych osobowych	Wyrok WSA - Oddalono skargę
171	2016-08-09 II SAB/Wa 1127/15	DOLiS-440-1360/13	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
172	2016-08-12 II SA/Wa 337/16	DOLiS/DEC-960/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
173	2016-08-18 I OSK 864/16	DOLiS/DEC-1016/14	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 8 września 2015 r. (II SA/Wa 34/15) w sprawie ze skargi na decyzję	Wyrok NSA - Oddalono skargę kasacyjną

			w przedmiocie przetwarzania danych osobowych	
174	2016-08-18 I OSK 86/16	DOLiS-440-646/13	Skarga kasacyjna od wyroku WSA w Warszawie z dnia 8 września 2015 r. (II SAB/Wa 644/14) w sprawie ze skargi na bezczynność w przedmiocie rozpoznania wniosku o ponowne rozpatrzenie sprawy	Wyrok NSA - Oddalono skargę kasacyjną
175	2016-08-19 II SAB/Wa 429/16	DOLiS-440-334/13	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
176	2016-08-19 II SAB/Wa 447/16	DOLiS-440-356/13	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA - Odrzucono skargę
177	2016-08-24 II SAB/Wa 180/16	DOLiS-440-1128/15	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono przewlekłość postępowania administracyjnego i że przewlekłość postępowania miała charakter rażący
178	2016-08-24 II SAB/Wa 1163/15	DOLiS-440-285/15	Skarga na bezczynność organu	Wyrok WSA - Oddalono skargę
179	2016-08-26 II SA/Wa 124/16	DOLiS/DEC-894/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
180	2016-09-02 II SA/Wa 1010/16	DOLiS/DEC-246/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
181	2016-09-06 II SA/Wa 830/15	DOLiS/POST-83/15	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku o kopię akt	Postanowienie WSA - Przywrócono termin do wniesienia skargi kasacyjnej
182	2016-09-06 II SA/Wa 1316/16	DOLiS/DEC-387/16	Skarga na decyzję w przedmiocie ochrony danych osobowych	Postanowienie WSA - Odrzucono skargę

183	2016-09-07 II SA/Wa 900/16	DOLiS/DEC-575/15	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Postanowienie WSA - Odrzucono skargę
184	2016-09-07 VIII SAB/Wa 151/15	DOLiS-440-995/12	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA - Odrzucono skargę
185	2016-09-14 II SA/Wa 926/16	DOLiS/POST-82/16	Skarga na postanowienie w przedmiocie wszczęcia postępowania	Wyrok WSA - Oddalono skargę
186	2016-09-14 II SAB/Wa 173/16	DOLiS-440-458/13	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono przewlekłość postępowania administracyjnego i że przewlekłość postępowania nie miała charakteru rażącego
187	2016-09-20 II SAB/Wa 608/16	DOLiS-440-409/15	Skarga na bezczynność organu	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
188	2016-09-20 II SA/Wa 1478/16	DOLiS/DEC-545/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odmówiono wstrzymania wykonania zaskarżonej decyzji
189	2016-09-23 II SA/Wa 595/16	DOLiS/DEC-116/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
190	2016-09-29 II SA/Wa 2199/15	DOLiS/DEC-828/15	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Postanowienie WSA - Odmówiono sporządzenia uzasadnienia
191	2016-09-29 II SA/Wa 392/16	DOLiS/DEC-985/15	Skarga na decyzję w przedmiocie udostępnienia danych osobowych	Wyrok WSA - Oddalono skargę
192	2016-09-30 II SAB/Wa 196/16	DOLiS-440-1628/14	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
193	2016-09-30 I OZ 978/16	DOLiS/DEC-118/16	Zażalenie na postanowienie WSA w Warszawie z dnia 16 czerwca 2016 r. (II SA/Wa 654/16) o odrzuceniu skargi w sprawie	Postanowienie NSA - Oddalono zażalenie

			ze skargi na decyzję w przedmiocie ochrony danych osobowych	
194	2016-10-03 II SA/Wa 1574/16	DOLiS/DEC-549/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Wstrzymano wykonanie zaskarżonej decyzji
195	2016-10-07 II SA/Wa 1426/16	DOLiS/DEC-495/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
196	2016-10-12 II SA/Wa 540/16	DOLiS-440-978/15	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
197	2016-10-12 II SA/Wa 305/16	DOLiS-440-1463/13	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę
198	2016-10-13 II SAB/Wa 336/16	DOLiS-440-725/12	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono przewlekłość postępowania administracyjnego i że przewlekłość postępowania miała charakter rażący oraz wymierzono grzywnę
199	2016-10-13 II SAB/Wa 1133/15	DOLiS-440-46/13	Skarga na przewlekłe prowadzenie postępowania	Wyrok WSA - Stwierdzono przewlekłość postępowania administracyjnego i że przewlekłość postępowania miała charakter rażący oraz wymierzono grzywnę
200	2016-10-13 II SA/Wa 1413/16	DOLiS/DEC-488/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
201	2016-10-14 I OSK 2920/15	DOLiS-440-213/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 20	Wyrok NSA - Uchylono zaskarżony wyrok

			maja 2015 r. (II SAB/Wa 979/14) w sprawie ze skargi na bezczynność w przedmiocie rozpoznania skargi na przetwarzanie danych osobowych	w części i w tym zakresie umorzono postępowanie, w pozostałym zakresie oddalono skargę kasacyjną
202	2016-10-19 II SA/Wa 526/16	DOLiS/POST-25/16	Skarga na postanowienie w przedmiocie zwrotu skargi z uwagi na nieuiszczenie opłaty skarbowej	Wyrok WSA - Oddalono skargę
203	2016-10-19 II SAB/Wa 341/16	DOLiS-440-1788/14	Skarga na bezczynność organu	Wyrok WSA - Zobowiązano do rozpatrzenia wniosku o ponowne rozpatrzenie sprawy i stwierdzono, że bezczynność organu miała miejsce z rażącym naruszeniem prawa, oraz wymierzono organowi grzywnę
204	2016-10-19 II SAB/Wa 585/16	DOLiS-440-1448/15	Skarga na przewlekłe prowadzenie postępowania	Postanowienie WSA - Odrzucono skargę
205	2016-10-20 II SAB/Wa 419/16	DOLiS-440-752/15	Skarga na bezczynność organu	Wyrok WSA - Stwierdzono bezczynność postępowania i że bezczynność nie miała miejsca z rażącym naruszeniem prawa
206	25.10.2016r. I OSK 1912/16	DIS/POST-475/15/94665 DIS-K-421/125/15	Skarga kasacyjna na postanowienie GIODO o kontynuowaniu kontroli.	oddalenie skargi kasacyjnej
207	2016-10-26 II SAB/Wa 191/16	DOLiS-440-1253/14	Skarga na bezczynność organu	Wyrok WSA - Zobowiązano do rozpatrzenia sprawy i stwierdzono, że bezczynność miała miejsce z rażącym naruszeniem prawa
208	2016-10-28 II SAB/Wa 645/16	DOLiS-440-84/15	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę

209	2016-11-07 II SAB/Wa 569/16	DOLiS-440-863/16	Skarga na bezczynność organu	Wyrok WSA - Oddalono skargę
210	2016-11-08 II SA/Wa 527/16	DOLiS/DEC-65/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
211	2016-11-16 II SA/Wa 1075/16	DOLiS/DEC-299/16	Skarga na decyzję w przedmiocie odmowy udostępnienia danych osobowych	Wyrok WSA - Uchylono zaskarżoną decyzję i poprzedzającą ją decyzję
212	2016-11-18 II SAB/Wa 575/16	DOLiS-035-3972/14	Skarga na bezczynność organu	Wyrok WSA - Zobowiązano do rozpatrzenia wniosku i stwierdzono, że bezczynność miała miejsce z rażącym naruszeniem prawa
213	2016-11-18 I OZ 1297/16	DOLiS/DEC-332/16	Zażalenia na postanowienie WSA w Warszawie z dnia 2 sierpnia 2016 r. (II SA/Wa 1111/16) o odmowie wstrzymania wykonania zaskarżonej decyzji w sprawie ze skargi na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie NSA - Uchylono zaskarżone postanowienie i przekazano sprawę do ponownego rozpoznania przez WSA
214	22.11.2016r. II SA/Wa 517/16	DIS/DEC-55/16/4756	Przetwarzanie danych osobowych zawartych w dokumentach tożsamości bez podstawy prawnej.	uchylenie decyzji
215	2016-11-22 II SAB/Wa 445/16	DOLiS-440-1126/15	Skarga na bezczynność organu	Wyrok WSA - Oddalono skargę
216	23.11.2016r. II SA/Wa 1639/16	DIS/DEC-587/16/62309	Usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez dopełnienie wobec osób, których dane pochodzące ze źródeł powszechnie dostępnych	odrzucenie skargi

			(Monitor Sądowy i Monitor Gospodarczy) zostały zebrane i utrwalone obowiązku informacyjnego,	
217	23.11.2016r. II SA/Wa 781/16	DIS/DEC-276/16/2295	Usunięcie uchybień poprzez: Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych przesyłanych za pomocą formularza kontaktowego ujawnij. pl. Opracowanie i wdrożenie dokumentacji przetwarzania danych. Wyznaczenie administratora bezpieczeństwa informacji. Nadanie osobom dopuszczonym do przetwarzania danych upoważnień do przetwarzania danych osobowych. Opracowanie ewidencji osób upoważnionych do przetwarzania danych. Określenie w umowie zawartej z Grupa Gram Sp.z o.o. Zakresu i celu powierzenia przetwarzania danych osobowych przetwarzanych w ramach portalu ujawnij.pl	oddalenie skargi
218	2016-11-24 II SAB/Wa 567/16	DOLiS-440-804/13	Skarga na bezczynność organu	Postanowienie WSA - Umorzono postępowanie z art. 161 ustawy p.p.s.a.
219	2016-11-25 II SA/Wa 1023/16	DOLiS/DEC-298/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Wyrok WSA - Oddalono skargę

220	2016-11-29 II SA/Wa 1009/16	DOLiS/DEC- 251/16	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Wyrok WSA - Uchy- lono zaskarżoną decy- zję i poprzedzającą ją decyzję
221	2016-11-29 I OSK 2220/15	DOLiS/DEC- 842/14	Skarga kasacyjna GIODO od wyroku WSA w Warszawie z dnia 21 kwietnia 2015 r. (II SA/Wa 1865/14) w spra- wie ze skargi na decyzję w przedmiocie przetwa- rzania danych	Postanowienie NSA - Umorzono postępowa- nie z art. 161 ustawy p.p.s.a.
222	2016-11-29 II SA/Wa 1749/16	DOLiS-440- 1270/11	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA - Wstrzymano wykona- nie zaskarżonej decy- zji
223	2016-11-30 II SA/Wa 1125/16	DOLiS/POST- 123/16	Skarga na postanowienie w przedmiocie odmowy uwzględnienia wniosku o sprostowanie decyzji	Wyrok WSA - Odda- lono skargę
224	2016-12-07 II SA/Wa 366/16	DOLiS/DEC-38/16	Skarga na decyzję w przedmiocie przetwa- rzania danych osobo- wych	Postanowienie WSA - Odrzucono skargę
225	2016-12-08 II SAB/Wa 566/16	DOLiS-440- 804/13	Skarga na bezczynność organu	Postanowienie WSA - Umorzono postępowa- nie z art. 161 ustawy p.p.s.a.
226	2016-12-09 II SAB/Wa 246/16	DOLiS-440- 816/15	Skarga na przewlekłe prowadzenie postępowa- nia	Wyrok WSA - Stwier- dzono przewlekłość postępowania admini- stracyjnego i że prze- wlekłość postępowania nie miała charakteru rażącego
227	2016-12-15 II SAB/Wa 552/16	DOLiS-440- 1611/14	Skarga na przewlekłe prowadzenie postępowa- nia	Wyrok WSA - Stwier- dzono przewlekłość postępowania admini- stracyjnego i że prze- wlekłość postępowania miała charakter rażący oraz wymierzono grzywnę

228	2016-12-16 II SA/Wa 2067/16	DOLiS/DEC-216/16	Skarga na decyzję w przedmiocie przetwarzania danych osobowych	Postanowienie WSA - Odrzucono skargę
229	2016-12-19 II SA/Wa 385/16	DOLiS/POST-522/15	Skarga na postanowienie w przedmiocie odmowy przywrócenia terminu do wniesienia wniosku o ponowne rozpatrzenie sprawy	Wyrok WSA - Stwierdzono nieważność zaskarżonego postanowienia
230	2016-12-28 II SAB/Wa 415/16	DOLiS-440-105/16	Skarga na bezczynność organu	Postanowienie WSA - Odrzucono skargę
231	2016-12-28 II SA/Wa 1749/16	DOLiS/DEC-680/16	Skarga na decyzję w przedmiocie nakazania udostępnienia danych osobowych	Postanowienie WSA - Zawieszono postępowanie

Załącznik nr 5

Wykaz wydarzeń objętych patronatem Generalnego Inspektora Ochrony Danych Osobowych w 2016 r.

1. Konferencja „KNOW HEALTH Cyber Security". Organizator: Data Techno Park Sp. Z o.o. Wrocław, 14 grudnia 2016 r.
2. Konferencja pt. „Działalność biznesowa w świetle nowych przepisów o ochronie danych osobowych". Organizator: Centrum Edukacji Menedżerskiej Uniwersytetu Ekonomicznego w Poznaniu. Poznań, 2 grudnia 2016 r.
3. Program edukacyjny dla MŚP w zakresie ochrony danych osobowych. Organizatorzy: Krajowa Izba Gospodarcza oraz Facebook.
4. Ogólnopolska Konferencja „Forum Bezpieczeństwa IT w Administracji". Organizatorzy: Redakcja miesięcznika „IT w Administracji" oraz Redakcja kwartalnika „ABI Expert". Gdańsk, 17-18 listopada 2016 r.
5. IV międzynarodowa Konferencja i Wystawa „Cyber Security – bezpieczeństwo ponad granicami". Organizator: Zarząd Targów Warszawskich S.A. Warszawa, 17 listopada 2016 r.
6. V Konwent Ochrony Danych i Informacji. Organizatorzy: ForSafe Sp. Z o.o. oraz Lubasz i Wspólnicy Kancelaria Radców Prawnych. Łódzka Specjalna Strefa Ekonomiczna, Łódź, 15 listopada 2016 r.
7. VI Mazowiecki Konwent Informatyków. Organizator: Redakcja miesięcznika „IT w Administracji". Warszawa, 27-28 października 2016 r.
8. Sesja „Forum Młodych Mistrzów – ekonomiczne aspekty informatyzacji Państwa" oraz patronat GIODO nad nagrodą za najlepszą prezentację z zakresu ochrony danych osobowych, przyznawaną podczas XXII Forum Teleinformatyki pt. „Państwo w cyberprzestrzeni – od izolacji do współdziałania". Miedzeszyn, 29-30 września 2016 r.
9. Konferencja dedykowana środowisku oświatowemu nt. kultury nauczania w środowisku cyfrowym oraz pozycja nauczyciela wobec wyzwań społeczeństwa informacyjnego. Organizator: Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Wydział Zamiejscowy WSB w Krakowie. Kraków, 17 września 2016 r.
10. III edycja Konferencji „Security Case Study 2016". Organizator: Fundacja Bezpieczna Cyberprzestrzeń. Warszawa, 14-15 września 2016 r.
11. GIODO w Komitecie Honorowym 14. Bałtyckich Targów Militarnych BALT-MILITARY-EXPO. Gdańsk, Centrum Wystawienniczo-Kongresowe AMBEREXPO, 20-22 czerwca 2016 r.
12. Ogólnopolski Konwent Informatyków. Organizator: Redakcja „IT w Administracji". Jarnołtówek, 9-10 czerwca 2016 r.
13. X Forum IAB. Organizator Związek Pracodawców Branży Internetowej IAB Polska. Warszawa, 8-9 czerwca 2016 r.
14. Konferencja „Udostępnianie wyników badań klinicznych – przywilej czy obowiązek?", zorganizowana z okazji obchodów Międzynarodowego Dnia Badań Klinicznych. Organizatorzy: Wydział Lekarski Collegium Medicum Uniwersytetu. Jagiellońskiego, Polska Filia Cochrane UJCM, Dział

Kliniczny, Sekcja ds. badań klinicznych UJCM. Międzynarodowe Centrum Kultury w Krakowie, 20 maja 2016 r.

15. XX Forum ADO/ABI. Organizator: Centrum Promocji Informatyki. Warszawa, 17 maja 2016 r.
16. II Ogólnopolski Kongres Zarządzania Ciągłością Działania. Organizator: BCMG. Warszawa, 13 maja 2016 r.
17. V Pomorski Konwent Informatyków. Organizatorzy: Redakcja „IT w Administracji". Jurata, 12-13 maja 2016 r.
18. Międzynarodowe Targi Zabezpieczeń SECUREX odbywające się w ramach Międzynarodowych Targów Poznańskich. Poznań, 25-28 kwietnia 2016 r.
19. Program edukacyjny dla MŚP w zakresie ochrony danych osobowych. Organizatorzy: Krajowa Izba Gospodarcza oraz Facebook.
20. IX edycja Ogólnopolskiego Konkursu ITelect. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Poland. 20 kwietnia - 18 maja 2016 r.
21. III Forum IT dla Kierowników w Administracji. Organizator: Redakcja miesięcznika „IT w Administracji". Zakopane, 20-22 kwietnia 2016 r.
22. VI Konferencja Naukowa „Ataki Sieciowe 2016". Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii, działające na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu. Toruń, 5-6 kwietnia 2016 r.
23. GIODO członkiem Komitetu Honorowego Obchodów Światowego Dnia Społeczeństwa Informacyjnego w Polsce w 2016 r. Organizator: Polskie Towarzystwo Informatyczne.
24. Konferencja „Pracodawca w przededniu reformy europejskiego prawa ochrony danych osobowych – z bagażem dotychczasowych zaniechań i wątpliwości". Organizator: Katedra Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego. Kraków, Auditorium Maximum UJ, 3 marca 2016 r.
25. Ogólnopolska kampania społeczna na rzecz bezpieczeństwa w sieci zorganizowana w ramach obchodów Międzynarodowego Dnia Ochrony Danych Osobowych – 28 stycznia. Organizatorzy: Śląska Sieć Metropolitarna, Miasto Gliwice, Gliwicki Ośrodek Metodyczny. Gliwice, Warszawa, Poznań, Kraków, Katowice, Wrocław, Opole, Bydgoszcz, Gdańsk. Styczeń 2016 r.

Załącznik nr 6

Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem GIODO lub jego przedstawicieli, zorganizowanych w 2016 r. W Polsce przez Generalnego Inspektora Ochrony Danych Osobowych lub inne podmioty.

l.p.	Data	Konferencja/Seminarium	Miejsce
1.	13.01.2016	Konferencja nt. przetwarzania danych w sektorze służby zdrowia. Organizatorzy: Generalny Inspektor Ochrony Danych Osobowych oraz Uniwersytet Śląski w Katowicach.	Katowice
2.	14.01.2016	Konferencja dt. ochrony danych osobowych w sektorze marketingu bezpośredniego. Organizatorzy: Generalny Inspektor Ochrony Danych Osobowych oraz Wyższa Szkoła Biznesu w Dąbrowie Górniczej.	Dąbrowa Górnicza
3.	19.01.2016	Konferencja pt. „Kradzież tożsamości”. Organizatorzy: Generalny Inspektor Ochrony Danych Osobowych oraz Wyższa Szkoła Policji w Szczytnie.	Szczytno
4.	28.01.2016	Konferencja nt. ochrony danych osobowych w Big Data. Organizatorzy: Generalny Inspektor Ochrony Danych Osobowych oraz Wydział Prawa i Administracji Uniwersytetu Warszawskiego.	Warszawa
5.	23.02.2016	Konferencja pt. „Administrator Bezpieczeństwa Informacji gwarantem właściwego stosowania przepisów o ochronie danych osobowych”. Organizatorzy: Generalny Inspektor Ochrony Danych Osobowych oraz Akademia Leona Koźmińskiego.	Warszawa
6.	25.02.2016	Konferencja nt. przetwarzania danych osobowych przez kościoły i związki wyznaniowe. Organizatorzy: Generalny Inspektor Ochrony Danych Osobowych oraz Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.	Warszawa

7.	9.03.2016	Sesja ekspercka w Miasteczku Orange pt. „Ochrona czy obrona? Bezpieczna cyberprzestrzeń”. Organizatorzy: Ośrodek Dialogu i Analiz THINKTANK oraz Orange Polska.	Warszawa
8.	10.03.2016	Konferencja pt. „Nowa regulacja przetwarzania danych osobowych – skutki w sektorze bankowym”. Organizator: Związek Banków Polskich.	Warszawa
9.	15.03.2016	Spotkanie Grupy Roboczej ds. Telekomunikacji, Mediów i Technologii, działającej w ramach British-Polish Chamber of Commerce pt. „ Nowe przepisy unijne w sprawie ochrony danych osobowych – co nas czeka z punktu widzenia praktyków i jak widzi to GIODO”. Organizator: British-Polish Chamber of Commerce.	Warszawa
10.	16.03.2016	Debata z okazji Światowego Dnia Konsumenta pn. „Konsument na rynku usług telekomunikacyjnych oraz e-commerce”. Organizator: Urząd Ochrony Konkurencji i Konsumentów.	Warszawa
11.	18.03.2016	III Konferencja Naukowa pt. „Telemedycyna w Polsce” z sesją specjalną nt. rejestrów medycznych w Polsce. Organizator: Wydawnictwo PRO MEDICINA.	Warszawa
12.	22-23.03.2016	IV międzynarodowy Kongres Płatności Bezgotówkowych. Organizator: Fundacja Rozwoju Obrotu Bezgotówkowego.	Warszawa
13.	1.04.2016	Konferencja Naukowa „Wpływ e-zdrowia na jakość i koszty opieki zdrowotnej”. Organizator: Polskie Towarzystwo Ekonomiki Zdrowia.	Warszawa
14.	5-6.04.2016	VI Konferencja Naukowa „Ataki Sieciowe 2016”. Organizator: Studenckie Koło Naukowe Prawa Nowych Technologii działające na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu.	Toruń
15.	7.04.2016	V Łódzki Konwent Informatyków. Organizator: Redakcja „IT w Administracji”.	Stryków
16.	8.04.2016	Międzynarodowa Konferencja New York State Bar Association (NYSBA).	Kraków

17.	14.04.2016	Forum Banków Spółdzielczych. Organizator: Polski Instytut Rozwoju Biznesu.	Warszawa
18.	19-22.04.2016	XIII Konferencja Szkoleniowo-Organizacyjna SAWS pod hasłem: „Archiwa resortu sprawiedliwości w obliczu zmian w przepisach prawnych". Organizator: Stowarzyszenie Archiwistów Instytucji Wymiaru Sprawiedliwości.	Warszawa
19.	20-22.04.2016	III Forum Kierowników IT w Administracji. Organizator: Redakcja „IT w Administracji".	Zakopane
20.	27.04.2016	Wystąpienie otwierające Konferencję „SECUREX BeIN" podczas 21. Edycji Międzynarodowych Targów Zabezpieczeń SECUREX. Organizator: Międzynarodowe Targi Poznańskie.	Poznań
21.	9.05.2016	Konferencja pt. „Outsourcing w jednostkach publicznych – odpowiedzialność zarządzających". Organizatorzy: Centrum Informacji Naukowej i Biblioteki Akademickiej Uniwersytetu Śląskiego oraz Uniwersytetu Ekonomicznego w Katowicach.	Katowice
22.	10.05.2016	IV Kongres Polskiej Izby Ubezpieczeń, pt. „Klient – Regulator – Kapitał. Jak zapewnić wartość rynku ubezpieczeń w warunkach ciągłej zmiany?". Organizator: Polska Izba Ubezpieczeń.	Sopot
23.	12.05.2016	Konferencja „Badania i innowacje w obszarze bezpieczeństwa – wymiana międzynarodowych doświadczeń". Organizator: Polska Platforma bezpieczeństwa Wewnętrznego.	Warszawa
24.	12.05.2016	Debata w Domu Dziennikarza pt. „Bezpieczeństwo i wolność słowa w cyberprzestrzeni". Organizator: Instytut Staszica oraz Centrum Monitoringu Wolności Prasy.	Warszawa
25.	12-13.05.2016	Pomorski Konwent Informatyków. Organizator: Redakcja „IT w Administracji".	Jurata
26.	13.05.2016	II Ogólnopolski Kongres Zarządzania Ciągłością Działania. Organizator: BCMG.	Warszawa

27.	14.05.2016	Konferencja „Inwigilacja, ile można?". Organizator: Naczelna Rada Adwokacka oraz Komisja Praw Człowieka działająca przy Naczelnej Radzie Adwokackiej.	Warszawa
28.	16.05.2016	Warsztat „Międzynarodowe doświadczenia w zakresie wykorzystania i ochrony administracyjnych danych osobowych". Organizatorzy: Ministerstwo Rozwoju i Bank Światowy.	Warszawa
29.	16.05.2016	Okrągły Stół pn. „Innowacje w sektorze finansowym – gdzie będziemy za 10 lat?" Organizator: Ośrodek Dialogu i Analiz THINKTANK.	Warszawa
30.	17.05.2016	XX Forum ADO/ABI. Organizator: Centrum Promocji Informatyki.	Warszawa
31.	19.05.2016	Debata pt. Bezpieczeństwo i wolność słowa w cyberprzestrzeni", zorganizowanej w Domu Dziennikarza. Organizator: Instytut Staszica oraz centrum Monitoringu Wolności Prasy.	Warszawa
32.	20.05.2016	VIII Konferencja Naukowa „ Bezpieczeństwo w Internecie" w ramach projektu badawczo-rozwojowego pn. „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym". Organizatorzy: UKSW, Narodowe Centrum Badań i Rozwoju, Narodowe Centrum Informatyczne.	Warszawa
33.	20.05.2016	Konferencja pt. „Udostępnianie wyników badań klinicznych – przywilej czy obowiązek?", zorganizowana z okazji Międzynarodowego Dnia Badań Klinicznych. Organizatorzy: OPS – Polska Filia Cochrane UJCB, Wydział Lekarski UJ-Collegium Medicum, Dział kliniczny, Sekcja ds. badań klinicznych UJ-CM.	Kraków
34.	24.05.2016	Spotkanie Grupy Roboczej ds. Telekomunikacji, Mediów i Technologii działającej w ramach British-Polish Chamber of Commerce (BPCC).	Wrocław
35.	7.06.2016	Seminarium podsumowujące VI edycją Ogólnopolskiego Programu Edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Organizator: GIODO	Warszawa

36.	8.06.2016	Konferencja pt. „Technologie biometryczne w Polsce – rozwój i zastosowanie". Organizator: Polski Instytut Rozwoju Biznesu (PIRB).	Warszawa
37.	10.06.2016	I Ogólnopolski Konwent Informatyków. Organizator: Redakcja „IT w Administracji".	Jarnołtówek
38.	16.06.2016	X Konferencja Hospital Management 2016 i debata ekspercka „Koordynowana opieka zdrowotna a dane wrażliwe związane z udzielaniem świadczeń – elektroniczna faktura, elektroniczna dokumentacja medyczna".	Warszawa
39.	20.06.2016	V Warmińsko-Mazurski Konwent Informatyków. Organizator: Redakcja „IT w Administracji".	Mrągowo
40.	22.06.2016	Wspólne posiedzenie seminaryjne Komisji Spraw Zagranicznych i Unii Europejskiej oraz Komisji Praw Człowieka, Praworządności i Petycji Senatu RP we współpracy z GIODO.	Warszawa
41.	24.06.2016	Konferencja pt. „Innowacyjna gospodarka oparta na danych". Organizator: ThinkTank Cyfrowy.	Warszawa
42.	29.06.2016	Konferencja pt. „Inspektor ochrony danych – kontynuator administratora bezpieczeństwa informacji czy nowa funkcja zapewniająca przestrzeganie przepisów o ochronie danych osobowych?". Organizator: Instytut Nauk Prawnych PAN.	Warszawa
43.	19.07.2016	Spotkanie związane z projektem Erasmus+ „Współpraca na rzecz innowacji i wymiany dobrych praktyk w dziedzinie szkolnictwa wyższego".	Warszawa
44.	8.09.2016	Spotkanie Dyrektorów Generalnych Urzędów Wojewódzkich.	Gdańsk
45.	9.09.2016	Warsztaty szkoleniowe dt. aktualnie obowiązujących i przyszłych zasad ochrony danych osobowych przewidzianych w ogólnym rozporządzeniu o ochronie danych osobowych. Organizator: Burmistrz Miasta Władysławowo.	Władysławowo
46.	13.09.2016	Debata ekspercka pt. „Europejskie rozporządzenie o ochronie danych. Co nas czeka, jak się	Warszawa

		przygotować? Organizator: Polska Press, Redakcja dziennika „Polska the Times”.	
47.	14-15.09.2016	Konferencja Szkoleniowa na UMCS w Lublinie pt. „Ochrona danych osobowych w świetle przepisów Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Stan aktualny i przyszłe rozwiązania” oraz w Lubelskim Urzędzie Wojewódzkim. Organizator: GIODO, UMCS oraz Lubelski Urząd Wojewódzki.	Lublin
48.	21.09.2016	Spotkanie z przedstawicielami Komisji Europejskiej. Organizatorzy: GIODO we współpracy z Przedstawicielstwem Komisji Europejskiej w Polsce.	Warszawa
49.	22.09.2016	XII Konferencja „BIOMETRIA 2016”. Organizatorzy: Politechnika Warszawska, Instytut Maszyn Matematycznych.	Warszawa
50.	22.09.2016	Międzynarodowa Konferencja „TRUSTED ID SUMMIT” – Nowe możliwości weryfikacji tożsamości klienta. Organizator: Medien Service.	Warszawa
51.	27.09.2016	Konferencja „Nowe oblicze bankowości – wykorzystanie technologii, bezpieczeństwo transakcji elektronicznych”. Organizator: SuccessPoint.	Warszawa
52.	29-30.09.2016	XXII Forum Teleinformatyki pt. „Państwo w cyberprzestrzeni – od izolacji do współdziałania”. Organizator BizTech Konsulting S.A.	Miedzeszyn
53.	4.10.2016	Konferencja „Funkcjonowanie BIG DATA po wejściu w życie rozporządzenia ogólnego w zakresie ochrony danych osobowych”. Organizator: Związek Banków Polskich.	Warszawa
54.	11.10.2016	Konferencja „Nowe regulacje w zakresie ochrony danych osobowych w sektorze finansowym”. Organizator: MMC Polska.	Warszawa
55.	15.10.2016	Inauguracja 2. edycji studiów podyplomowych pn. „Wykonywanie funkcji Administratora Bezpieczeństwa Informacji i Inspektora Ochrony Danych” w INP PAN.	Warszawa

56.	18.10.2016	Warsztaty zarządzania Internetem „Sprawdź kto rządzi Internetem. Internet dzisiaj i jutro". Organizatorzy: Ministerstwo Cyfryzacji, Internet Corporation for Assigned Names and Numbers (ICANN), Naukowa i Akademicka Sieć Komputerowa (NASK) oraz Digital Economy Lab Uniwersytetu Warszawskiego.	Warszawa
57.	25-26.10.2016	XX Konferencja nt. bezpieczeństwa teleinformatycznego SECURE 2016. Organizator: NASK.	Warszawa
58.	27-28.10.2016	IV Mazowiecki Konwent Informatyków. Organizator: Redakcja „IT w Administracji".	Ołtarzew k/Warszawy
59.	15.11.2016	Konferencja „Prawa dziecka w konstelacji rodzinnej i placówek oświatowych" w ramach cyklu konferencji o prawach dziecka w obszarach społecznych. Organizatorzy: GIODO, UKSW w Warszawie, Rzecznik Praw Dziecka.	Warszawa
60.	15.11.2016	V Konwent Ochrony Danych Osobowych i Informacji. Organizatorzy: Lubasz i Wspólnicy Kancelaria Radców Prawnych oraz ForSafe Sp. Z o.o.	Łódź
61.	16.11.2016	Konferencja „Trusted Cloud Day 2016".	Warszawa
62.	18.11.2016	Konferencja z okazji Jubileuszu 200-lecia Prokuratorii Generalnej. Organizator: Prokuratoria Generalna Skarbu Państwa.	Warszawa
63.	21.11.2016	Seminarium GDPR dt. cyberbezpieczeństwa. Organizator: Ambasada Brytyjska w Warszawie.	Warszawa
64.	22.11.2016	Konferencja „Kradzież tożsamości w Internecie". Organizatorzy: GIODO, Ministerstwo Spraw Wewnętrznych i Administracji, Wydział Administracji i Nauk Społecznych Politechniki Warszawskiej.	Warszawa
65.	23.11.2016	XI Forum Kierowników Jednostek Organizacyjnych oraz Pełnomocników ds. Ochrony Informacji Niejawnych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.	Zakopane
66.	24.11.2016	Międzynarodowa Konferencja pt. „Drony jako źródło nowych miejsc pracy i wzrostu gospodarczego".	Warszawa

67.	28.11.2016	XI Forum Nowej Gospodarki „Lokalna energia 2016". Organizator: Akademia Górniczo-Hutnicza.	Kraków
68.	2.12.2016	Konferencja „Wpływ nowych unijnych przepisów o ochronie danych na działalność biznesową". Organizator: Centrum Edukacji Menedżerskiej Uniwersytetu Ekonomicznego w Poznaniu.	Poznań
69.	7.12.2016	Ogólnopolska Konferencja Naukowa „Wdrożenie ogólnego rozporządzenia o ochronie danych – aspekty proceduralne". Organizatorzy: GIODO, Prezes Naczelnego Sądu Administracyjnego, Dziekan Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.	Warszawa
70.	7.12.2016	II Konferencja Naukowa pt. "Bezpieczeństwo informacyjne w obszarze cyberprzestrzeni".	Gdynia
71.	14.12.2016	Konferencja „KNOW HEALTH Cyber Security". Organizator: Data Techno Park Sp. Z o.o.	Wrocław

Załącznik nr 7

Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem GIODO lub jego przedstawicieli, które odbyły się w 2016 r. Za granicą.

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	13-14.01.2016	Posiedzenie Podgrupy ds. Technologii.	Bruksela
2.	27-28.01.2016	Warsztaty w ramach projektu PHAEDRA II	Bruksela
3.	19-20.01.2016	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
4.	1-3.02.2016	104. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
5.	17-18.02.2016	Grupa nadzorująca zmianę podstaw prawnych Europolu.	Haga
6.	3-4.03.2016	Międzynarodowa Konferencja dt. edukacji dzieci i młodzieży z zakresu prawa do prywatności i ochrony danych osobowych, zorganizowana w ramach projektu ARCADES.	Barcelona
7.	8-9.03.2016	Posiedzenie Podgrupy ds. Technologii.	Bruksela
8.	9.03.2016	Agenda Cooperation Subgroup.	Bruksela
9.	9.03.2016	Posiedzenie Grupy Roboczej Prawników Lingwistów.	Bruksela
10.	14-18.03.2016	Misja ewaluacyjna.	Rzym
11.	15.03.2016	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
12.	15-16.03.2016	Warsztaty CIPL.	Amsterdam
13.	29-30.03.2016	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
14.	31.03.2016	Posiedzenie Wspólnego Organu Nadzorczego Europolu.	Bruksela
15.	11-13.04.2016	Kick-off meeting w ramach programu ERASMUS+.	Sofia

16.	24-26.04.2016	59. posiedzenie Międzynarodowej Grupy Roboczej ds. Ochrony Danych Osobowych w Telekomunikacji (Grupa Berlińska). Misja ewaluacyjna Schengen.	Oslo
17.	10-13.05.2016	18. Spotkanie Grupy Państw Europy Środkowej i Wschodniej.	Sarajewo
18.	11-12.05.2016	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
19.	15-20.05.2016	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II).	Sofia
20.	17-18.05.2016	Posiedzenie Podgrupy ds. Współpracy, Grupy Roboczej Art. 29.	Bruksela
21.	23-24.05.2016	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
22.	25-27.05.2016	Wiosenna Konferencja Europejskich Rzeczników Ochrony Danych (European Conference of Data Protection Authorities).	Budapeszt
23.	6-8.06.2016	106. posiedzenie Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
24.	8-10.06.2016	Posiedzenie Wspólnych Organów Nadzorczych	Bruksela
25.	12-17.06.2016	Czynności kontrolne systemu informacyjnego Schengen.	Ryga
26.	13-14.06.2016	Grupa koordynująca nadzór nad IMI.	Bruksela
27.	22-23.06.2016	Posiedzenie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions).	Bruksela
28.	28.06.-1.07.2016	33. Posiedzenie Plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD).	Strasburg
29.	30.06.2016	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers).	Bruksela

30.	4-5.07.2016	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29.	Bruksela
31.	4-5.07.2016	Posiedzenie Podgrupy ds. Technologii.	Bruksela
32.	6.07.2016	Posiedzenie Podgrupy ds. Współpracy, Grupy Roboczej Art. 29.	Bruksela
33.	25-27.07.2016	Specjalne Posiedzenie Plenarne Grupy Roboczej Art. 29 ds. Ochrony Danych.	Bruksela
34.	26-27.07.2016	Warsztaty Grupy Roboczej Art. 29 ds. Ochrony Danych oraz warsztaty KE.	Bruksela
35.	16-20.10.2016	38. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności.	Marakesz
36.	31.08-02.09.2016	Warsztaty Grupy Roboczej Art. 29 oraz posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29	Bruksela
37.	19-20.09.2016	Warsztaty dt. Wdrożenia ogólnego rozporządzenia o ochronie danych	Paryż
38.	25-30.09.2016	Czynności kontrolne Systemu Informacyjnego Schengen (SIS II).	Budapeszt
39.	26-28.09.2016	107. posiedzenie Grupy Roboczej Art. 29.	Bruksela
40.	2-7.10.2016	Czynności kontrolne Systemu Informacyjnego Schengen (SIS II).	Bukareszt
41.	3-4.10.2016	Posiedzenie Wspólnego Organu Nadzorczego Europolu.	Bruksela
42.	4-5.10.2016	Spotkanie Organów Ochrony Danych Europy Środkowej	Vrakun
43.	12-15.10.2016	Międzynarodowe warsztaty rozpatrywania spraw.	Podgorica
44.	19-20.10.2016	Posiedzenie Podgrupy ds. Technologii.	Bruksela
45.	4.11.2016	Posiedzenie Podgrupy ds. Współpracy, Grupy Roboczej Art. 29.	Bruksela
46.	7.11.2016	Posiedzenie Podgrupy ds. e-Administracji, Grupy Roboczej Art. 29.	Bruksela
47.	7-9.11.2016	7. Międzynarodowa Konferencja o Ochronie Danych Osobowych.	Moskwa

48.	9-10.11.2016	Posiedzenie Podgrupy ds. Kluczowych Postanowień Dyrektywy (Key Provisions).	Bruksela
49.	14-15.11.2016	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
50.	16-17.11.2016	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers) Grupy Roboczej Art. 29.	Bruksela
51.	21-23.11.2016	Spotkanie grup koordynujących nadzór nad SIS, VIS i Eurodac.	Bruksela
52.	21-24.11.2016	60. Posiedzenie Grupy Berlińskiej oraz warsztaty dt. śledzenia online.	Berlin
53.	22.11.2016	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29.	Bruksela
54.	8-9.12.2016	Posiedzenie JSB (Europol) oraz posiedzenie JSA (Customs)	Bruksela
55.	12-13.12.2016	108. posiedzenie Grupy Roboczej Art. 29 oraz warsztaty projektu PHAEDRA II.	Bruksela
56.	14-15.12.2016	Konferencja Rady Europy dt. Wzmacniania ochrony danych osobowych w państwach Partnerstwa Wschodniego, zorganizowana w ramach „Programmatic Cooperation Framework (PCF).	Tbilisi
57.	19-20.12.2016	Spotkanie dt. oddelegowania eksperta narodowego do Europejskiego Inspektora Ochrony Danych Osobowych.	Bruksela