SPRAWOZDANIE Z DZIAŁALNOŚCI PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH W ROKU 2018

Sprawozdanie stanowi wykonanie art. 59 rozporządzenia 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)[1], zgodnie z którym każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu środków zgodnie z art. 58 ust. 2. Sprawozdania te są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem państwa członkowskiego. Są one udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych. Powołany przepis jest uzupełniony przez art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[2], w myśl którego Prezes Urzędu Ochrony Danych Osobowych[3] raz w roku, do dnia 31 sierpnia przedstawia Sejmowi RP, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności, zawierające w szczególności informację o liczbie i rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia Prezesa UODO oraz wnioski ze stanu przestrzegania przepisów o ochronie danych osobowych (ust. 1). Prezes UODO udostępnia sprawozdanie na swojej stronie podmiotowej Biuletynu Informacji Publicznej (ust. 2).

Sprawozdanie obejmuje działalność Prezesa UODO od 25 maja do 31 grudnia 2018 r. oraz działalność Generalnego Inspektora Ochrony Danych Osobowych[4], którego Prezes UODO jest następcą prawnym, od 1 stycznia do 24 maja 2018 r.

[1] Dz. Urz. UE L 119, z 4.5.2016, str. 1; sprostowanie Dz. Urz. UE L 127 z 23.5.2018, str. 2 - dalej jako: ogólne rozporządzenie o ochronie danych lub RODO, lub rozporządzenie 2016/679

[2] Dz. U. poz. 1000 z późn. zm.

[3] Dalej także jako Prezes UODO

[4] Dalej także jako GIODO

Spis treści

Szanowni Państwo,

zgodnie z ogólnym rozporządzeniem o ochronie danych oraz ustawą z 10 maja 2018 r. o ochronie danych osobowych, Prezes Urzędu Ochrony Danych Osobowych tak jak w latach poprzednich Generalny Inspektor Ochrony Danych Osobowych, raz do roku przedkłada Sejmowi RP sprawozdanie ze swojej działalności. Na mocy art. 50 ustawy o ochronie danych osobowych po raz pierwszy Prezes UODO przedkłada sprawozdanie także Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu.

W 2018 r. rozpoczęło się bezpośrednie stosowanie ogólnego rozporządzenia o ochronie danych, równocześnie została przyjęta oraz weszła w życie nowa ustawa o ochronie danych osobowych, która m.in. wprowadziła zmiany instytucjonalne w polskim systemie ochrony danych osobowych, zastępując GIODO Prezesem UODO.

Niniejsze sprawozdanie prezentuje najważniejsze ustalenia z realizowanych przez Prezesa UODO oraz GIODO w 2018 r. ustawowych zadań, wśród których wymienić należy: rozpatrywanie skarg obywateli, prowadzenie kontroli, opiniowanie projektów aktów prawnych, przyjmowanie zgłaszanie naruszeń ochrony danych, działalność edukacyjno-informacyjną, czy też uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Jest to pierwsze sprawozdanie przyjęte w nowych ramach prawnych i instytucjonalnych ochrony danych osobowych, które pokazuje najważniejsze problemy i wnioski związane z przełomowym okresem wdrażania nowych przepisów o ochronie danych osobowych. Okres ten obfitował w wiele wyzwań zarówno związanych z procesem niezbędnych zmian legislacyjnych, który niestety w 2018 r. jeszcze w pełni nie zakończył się, jak i z koniecznymi zmianami instytucjonalnymi i organizacyjnymi polskiego organu nadzorczego.

Zachęcam do lektury sprawozdania z działalności polskiego organu ochrony danych osobowych w roku 2018, którą to funkcję w tym czasie pełniła dr Edyta Bielak-Jomaa, jako ostatni GIODO oraz pierwszy Prezes UODO.

Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

I. WPROWADZENIE

1. Źródła prawa w zakresie ochrony danych osobowych

Podstawę prawną działania Prezesa UODO przede wszystkim stanowi ogólne rozporządzenie o ochronie danych oraz ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, a także wydane na jej podstawie akty wykonawcze:

- rozporządzenie Rady Ministrów z dnia 14 stycznia 2019 r. w sprawie wysokości wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym[5];
- rozporządzenie Rady Ministrów z dnia 20 marca 2019 r. w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych[6].

W 2016 r. w pakiecie legislacyjnym reformującym ramy prawne ochrony danych osobowych w UE oprócz RODO została także przyjęta 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[7]. Dyrektywa w odróżnieniu od rozporządzenia unijnego wymaga implementacji w prawie krajowym poprzez przyjęcie odpowiedniej ustawy. Zgodnie z postanowieniami dyrektywy 2016/680 wszystkie państwa członkowskie UE powinny ją wdrożyć do 6 maja 2018 r. W polskim systemie prawnym nastąpiło to z opóźnieniem, gdyż ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości została uchwalona dopiero 14 grudnia 2018 r.[8], a weszła w życie 6 lutego 2019 r.[9] Następnie na podstawie wskazanej ustawy z 14 grudnia 2018 r. zostało wydane rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych[10].

W związku z tym pomimo wejścia w życie 25 maja 2018 r. przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych i uchylenia wcześniejszej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[11], w zakresie zastosowania dyrektywy 2016/680 niektóre przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych zostały utrzymane w mocy. Zgodnie z art. 175 ustawy z 10 maja 2018 r. ustawy o ochronie danych osobowych art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziały 4, 5 i 7 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych zachowały moc w odniesieniu do przetwarzania danych osobowych przez właściwe organy i służby w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu do dnia wejścia w życie przepisów wdrażających dyrektywę 2016/680[12].

---

[5] Dz. U. poz. 164

[6] Dz. U. poz. 697

[7] Dz. Urz. UE L 119 z 04.05.2016, str. 89 – dalej jako dyrektywa 2016/680 lub dyrektywa policyjna.

[8] Dz. U. z 2019 r. poz. 125 – dalej także jako ustawa z 14 grudnia 2018 r. o ochronie danych osobowych lub u.o.d.o.z.z.

[9] Zgodnie z art. 18 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości jej art. 58 pkt 12 wejdzie w życie 1 listopada 2019 r., a art. 82 pkt 5 w zakresie art. 25c–25h wejdą w życie 23 stycznia 20120 r.

[10] Dz. U. poz. 1041, rozporządzenie weszło w życie 6 czerwca 2019 r.

[11] tj. Dz. U. z 2016 r. poz. 922 z późn. zm.

[12] Wskazane przepisy obowiązywały do 5 lutego 2019 r.

Zgodnie z art. 166 ust. 1 ustawy z 10 maja 2018 roku o ochronie danych osobowych z dniem 25 maja 2018 r. GIODO stał się Prezesem UODO, a na podstawie art. 167 ust. 1 powołanej ustawy Biuro GIODO – Urzędem Ochrony Danych Osobowych.
Zgodnie z art. 34 ust. 2 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Prezes UODO jest organem nadzorczym w rozumieniu:

- rozporządzenia 2016/679;
- dyrektywy 2016/680;
- rozporządzenia 2016/794[13].

Zgodnie z RODO do zadań Prezesa UODO należy:

- monitorowanie i egzekwowanie stosowania RODO;
- upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienia tych zjawisk (ze szczególną uwagą poświęconą działaniom skierowanym do dzieci);
- doradzanie, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych;
- upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO;
- udzielanie osobom, których dane dotyczą, na ich żądanie informacji o wykonywaniu praw przysługujących im na mocy RODO, a w stosowym przypadku współpraca w tym celu z organami nadzorczymi innych państw członkowskich UE;
- rozpatrywanie skarg wniesionych przez osoby, których dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80 RODO, w odpowiednim zakresie prowadzenie postępowania w przedmiocie tych skarg i w rozsądnym terminie informowanie skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem;
- współpraca z innymi organami nadzorczymi, w tym dzielenie się informacjami oraz świadczenie wzajemnej pomocy, w celu zapewnienia spójnego stosowania i egzekwowania RODO;
- prowadzenie postępowań w sprawie stosowania RODO, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
- monitorowanie zmian w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitorowanie rozwoju technologii informacyjno-komunikacyjnych i praktyk handlowych;
- przyjmowanie standardowych klauzul umownych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d RODO;
- ustanowienie i prowadzenie wykazu operacji podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4 RODO;
- udzielanie zaleceń, o których mowa w art. 36 ust. 2 RODO, dotyczących planowanych operacji przetwarzania danych;

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. Urz. UE L 135 z 24 maja 2016 r., str. 53) – dalej jako: rozporządzenie 2016/794.

- zachęcanie do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1 RODO, wydawanie opinii na ich temat oraz zatwierdzanie tych kodeksów, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5 RODO;
- zachęcanie do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny zgodnie z art. 42 ust. 1 RODO, a także zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5;
- gdy ma to zastosowanie – zgodnie z art. 42 ust. 7 RODO – dokonywanie okresowego przeglądu udzielonych certyfikacji;
- opracowywanie i publikacja wymogów akredytacji podmiotów monitorujących kodeksy postępowania na mocy art. 41 oraz podmiotów certyfikujących na mocy art. 43;
- akredytacja podmiotów monitorujących kodeksy postępowania zgodnie z art. 41 oraz podmiotów certyfikujących na mocy art. 43;
- wydawanie zezwoleń na klauzule umowne i uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 RODO;
- zatwierdzanie wiążących reguł korporacyjnych na mocy art. 47 RODO;
- udział w pracach Europejskiej Rady Ochrony Danych;
- prowadzenie wewnętrznego rejestru naruszeń ogólnego rozporządzenia o ochronie danych i działań podjętych zgodnie z art. 58 ust. 2 RODO;
- wypełnianie innych zadań związanych z ochroną danych osobowych.

Wraz z powyższymi zadaniami, Prezesowi UODO przysługuje wiele uprawnień. **Należą do nich m.in. uprawnienia Prezesa UODO w zakresie prowadzonych postępowań przyznane na mocy ogólnego rozporządzenia o ochronie danych:**

- nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;
- prowadzenie postępowań w formie audytów ochrony danych;
- dokonywanie przeglądu udzielonych certyfikacji na mocy art. 42 ust. 7 RODO;
- zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia RODO;
- uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;
- 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.

Do uprawnień naprawczych Prezesa UODO przyznanych na mocy RODO zalicza się:

- wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
- udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania;
- nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO;
- nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazanie sposobu i terminu;

- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
- nakazanie na mocy art. 16, 17 i 18 RODO sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
- cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43 RODO, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
- zastosowanie, oprócz lub zamiast środków, o których mowa w ogólnym rozporządzeniu o ochronie danych, administracyjnej kary pieniężnej na mocy art. 83 RODO, zależnie od okoliczności konkretnej sprawy;
- nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Uprawnienia Prezesa UODO w zakresie wydawania zezwoleń i uprawnienia doradcze przyznane na mocy RODO obejmują:

- udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 36 RODO;
- 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;
- zezwalanie na przetwarzanie zgodnie z art. 36 ust. 5 RODO, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;
- opiniowanie i zatwierdzanie projektów kodeksów postępowania zgodnie z art. 40 ust. 5 RODO;
- udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5;
- przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d RODO;
- zezwalanie na klauzule umowne, o których mowa w art. 46 ust. 3 lit. a RODO;
- zezwalanie na uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b RODO;
- zatwierdzanie wiążących reguł korporacyjnych na mocy art. 47 RODO.

Nie są to jedyne zadania i kompetencje należące do polskiego organu nadzorczego. Dodatkowe obowiązki Prezesa UODO wynikają również innych przepisów europejskich i krajowych. 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 RP, 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.

Do 24 maja 2018 r. podstawę prawną działania GIODO stanowiła ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych 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[14] i rozporządzenie

[14] Dz. U. z 2011 r. Nr 225, poz. 1350

Prezydenta Rzeczypospolitej Polskiej z dnia 19 listopada 2015 r. zmieniające rozporządzenie w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych;[15]

- 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[16];
- rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych[17];
- rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji[18];
- rozporządzenie z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych[19] 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[20];
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[21];
- 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[22].

Zadania i kompetencje GIODO wyznaczały przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. W ich świetle GIODO był 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[23],
- 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.

[15] Dz. U. z 2015 r. poz. 2020
[16] Dz. U. z 2015 r. poz. 745
[17] Dz. U. z 2015 r. poz. 719
[18] Dz. U. z 2014 r., poz. 1934
[19] Dz. U. Nr 94, poz. 923
[20] Dz. U. z 2011 r., Nr 103, poz. 601
[21] Dz. U. z 2008 r. Nr 229, poz. 1536
[22] Dz. U. z 2004 r., Nr 100, poz. 1024
[23] Tj. Dz. U. z 2019 r. poz. 1438

2. Urząd Ochrony Danych Osobowych

2.1. Struktura organizacyjna

UODO zapewnia wykonanie zadań wynikających z kompetencji Prezesa UODO określonych w rozporządzeniu 2016/679, ustawie o ochronie danych osobowych, a także w innych przepisach powszechnie obowiązującego prawa.

Organizację i zasady działania UODO określa statut stanowiący załącznik do zarządzenia nr 1/2018 Prezesa UODO z 25 maja 2018 r. w sprawie nadania statutu UODO[24]. Statutowymi komórkami organizacyjnymi UODO są:

1) Zespół Analiz i Strategii,
2) Zespół ds. Sektora Publicznego,
3) Zespół ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa,
4) Zespół ds. Sektora Organów Ścigania i Sądów,
5) Zespół Wstępnej Oceny Skarg,
6) Zespół ds. Sektora Prywatnego,
7) Zespół Współpracy Międzynarodowej i Edukacji,
8) Zespół Współpracy z Administratorami Danych,
9) Zespół Organizacyjny,
10) Zespół ds. Kar i Egzekucji,
11) Zespół ds. Certyfikacji i Monitorowania Kodeksów,
12) Zespół Prasowy,
13) Samodzielne Stanowisko Inspektora Ochrony Danych,
14) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych,
15) Zespół Administracyjny,
16) Zespół Informatyki,
17) Dział Kadr,
18) Dział Finansowy,
19) Zespół Radców Prawnych,
20) Dział Kontroli Wewnętrznej i Zarządczej.

Warto zauważyć, że do 24 maja 2018 r. tryb pracy Biura GIODO, a także organizację wewnętrzną i szczegółowy zakres zadań statutowych jednostek organizacyjnych Biura GIODO określał GIODO w regulaminie organizacyjnym. Natomiast statut Biuru GIODO nadawał Prezydent Rzeczypospolitej Polskiej, po zasięgnięciu opinii GIODO, w drodze rozporządzenia, 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 GIODO. Jak wskazano wcześniej w aktualnym stanie prawnym statut UODO nadaje jego Prezes.

2.2. Pracownicy UODO

Stan zatrudnienia w Biurze GIODO na dzień 1 stycznia 2018 r. w przeliczeniu na pełne etaty wynosił 161,65 etatu (tj. 165 osób). Zatrudnienie w UODO na dzień 31 grudnia 2018 r. wynosiło 232,25 etatu (tj. 235 osób). Na stanowiskach merytorycznych zatrudnionych było 194 osób, a na stanowiskach pomocniczych 39 osób. Wyższe wykształcenie posiadało 210 pracowników, w tym 122 legitymowało się wykształceniem wyższym prawniczym.

[24] Opublikowany 5 czerwca 2018 r. na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/p/statut-urzedu.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Biura GIODO na początku 2018 r. przedstawiała się następująco:

1) GIODO – 1 osoba,
2) Zastępca GIODO – 1 osoba,
3) Dyrektor Biura – 1 osoba,
4) Zespół Rzecznika Prasowego – 3 osoby,
5) Departament Edukacji Społecznej i Współpracy Międzynarodowej – 12 osób,
6) Departament Informatyki – 10 osób,
7) Departament Inspekcji – 24 osoby,
8) Departament Administracyjno-Techniczny – 18 osób,
9) Departament Orzecznictwa, Legislacji i Skarg – 58 osób,
10) Departament Rejestracji Administratorów, Bezpieczeństwa Informacji i Zbiorów Danych Osobowych – 19 osób,
11) Dział Finansowy – 3 osoby,
12) Zespół ds. Kadr i Organizacji – 4 osoby,
13) Zespół ds. Egzekucji Administracyjnej – 3 osoby,
14) Zespół Radców Prawnych – 3 osoby
15) Samodzielne Stanowisko ds. Audytu Wewnętrznego – 1 osoba (0,5 etatu),
16) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych –1 osoba,
17) Radca – samodzielne stanowisko – 1 osoba (1 etat).

Liczba pracowników zatrudnionych w poszczególnych komórkach organizacyjnych UODO na koniec 2018 r. kształtowała się następująco:

1) Prezes UODO – 1 osoba
2) Zastępca Prezesa UODO – 1 osoba
3) Dyrektor UODO – 1 osoba
4) Zespół Administracyjny – 24 osoby,
5) Zespół Analiz i Strategii – 10 osób,
6) Zespół Informatyki – 13 osób,
7) Zespół ds. Kar i Egzekucji – 8 osób,
8) Zespół Organizacyjny – 6 osób,
9) Zespół Prasowy – 5 osób,
10) Zespół Radców Prawnych – 3 osoby,
11) Zespół ds. Sektora Organów Ścigania i Sądownictwa – 15 osób,
12) Zespół ds. Sektora Prywatnego – 30 osób,
13) Zespół ds. Sektora Publicznego – 25 osób,
14) Zespół ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 19 osób (19 etatów),
15) Zespół Współpracy z Administratorami Danych – 24 osób,
16) Zespół Współpracy Międzynarodowej i Edukacji – 16 osób,
17) Zespół Wstępnej Oceny Skarg – 18 osób,
18) Dział Kadr – 3 osoby,
19) Dział Finansowy – 3 osoby (3 etaty),
20) Dział Kontroli Wewnętrznej i Zarządczej – 1 osoba (1 etat),
21) Samodzielne Stanowisko ds. Audytu Wewnętrznego – 1 osoba (1 etat),
22) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 1 osoba (1 etat),
23) Radca – samodzielne stanowisko - 1 osoba (1 etat).

2.3.Budżet UODO

Prezes UODO jest dysponentem głównym środków wydzielonych dla części 10 budżetu państwa:

1) dział 751 – Urzędy naczelnych organów władzy państwowej, kontroli i ochrony prawa oraz sądownictwa;
2) rozdział 75101 – Urzędy naczelnych organów władzy państwowej, kontroli i ochrony prawa.

Ustalony w ustawie budżetowej na 2018 r. budżet UODO po stronie wydatków wynosił 21 006 tys. zł. W planie finansowym na 2018 r. Prezes UODO określił wydatki :

- świadczenia na rzecz osób fizycznych – 15 tys. zł,
- wydatki bieżące – 20 191 tys. zł,
- wydatki majątkowe – 800 tys. zł.

Na podstawie przepisów art. 171 ust. 3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[25] Prezes UODO dokonał przeniesień między paragrafami klasyfikacji wydatków, w ramach części 10 (dział 751, rozdział 75101), na łączną kwotę 350 tys. zł.

W 2018 r. zwiększono plan UODO o kwotę 16 574 tys. zł, pochodzącą z rezerwy celowej (poz. 73), w tym:

- § 4000 – 1 738 tys. zł,
- § 4010 – 3 051 tys. zł,
- § 4110 – 525 tys. zł,
- § 4120 – 75 tys. zł,
- § 606 – 11 185 tys. zł.

Z ww. kwoty sfinansowano:

- wynagrodzenia i pochodne od wynagrodzeń (dla 106 osób zatrudnionych od 25 maja do 31 grudnia 2018 r.) – 2 750,1 tys. zł,
- zakupy materiałów i usług (komputery, biurka, szafy, wynajem powierzchni biurowej) – 1 719,6 tys. zł,
- wydatki majątkowe (programy, sprzęt informatyczny) – 569 tys. zł.

Niewykorzystana kwota 11 535,2 tys. zł została zwrócona Ministerstwu Finansów.

Wykonanie wydatków UODO w 2018 r. wyniosło 25 681 tys. zł, tj. 68,3 proc. planu ujętego w ustawie budżetowej. W porównaniu do 2017 r. wykonanie wydatków było wyższe o 5 531 tys. zł (27,4 proc.).

Struktura wydatków w 2018 r.

Grupa wydatków		Wydatki w tys. zł	Struktura %
I	Wynagrodzenia i pochodne	17 274	67,3
II	Wydatki rzeczowe	7 166	27,9
III	Zakupy majątkowe	1 006	3,9
IV	Odpis na ZFŚS	235	0,9
Ogółem		25 681	100

Środki finansowe określone w ustawie budżetowej na 2018 r. pozwoliły na realizację w I półroczu jedynie zadań takich jak w 2017 r.

[25] Tj. Dz. U. z 2019 r. poz. 869

Decyzją Ministra Finansów z 26 września 2018 r. plan wydatków w § 6060 został zwiększony o kwotę 11 185 tys. zł, pochodzącą z rezerwy celowej (cz. 83, dz. 758, rozdz. 75818, § 6800). Jednakże obowiązujące przepisy ustawy z dnia 29 stycznia 1994 r. - Prawo zamówień publicznych[26] oraz ustawy o finansach publicznych nie pozwalały na wszczęcie procedur przetargowych bez zabezpieczenia środków finansowych, a te ze względu na skomplikowane procedury związane z zakupem systemów informatycznych musiałyby być zapewnione na początku 2018 r**.** Z uwagi na powyższe uzależnienie uruchomienia rezerwy celowej od wejścia w życie 25 maja 2018 r. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych było główną przyczyną niezrealizowania planowanych zakupów informatycznych.

W ramach wydatków majątkowych sfinansowanych z rezerwy celowej (cz. 83, dz. 758, rozdz. 75818, § 6800) zakupiono:

- systemy informatyczne i licencje – 282 tys. zł,
- urządzenia sieciowe – 263 tys. zł,
- system kontroli dostępu – 24 tys. zł.

Natomiast w ramach wydatków majątkowych sfinansowanych z budżetu UODO zakupiono:

- systemy informatyczne i licencje – 25 tys. zł,
- urządzenia wielofunkcyjne – 163 tys. zł,
- macierz – 24 tys. zł,
- rozbudowa centrali telefonicznej – 25 tys. zł.

Łącznie wydatkowano w ramach § 6060 kwotę 1 006 tys. zł.

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI

1. Wprowadzenie

Każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo to zostało zagwarantowane w art. 51 Konstytucji RP, art. 8 Karty praw podstawowych UE, a także art. 16 Traktatu o funkcjonowaniu UE. Szczegółowe normy służące realizacji tego prawa wprowadza przede wszystkim rozporządzenie 2016/679, określając zasady przetwarzania danych, związane z tym obowiązki administratorów oraz prawa osób, których dane dotyczą.

Za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest taka, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

RODO stosuje się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz w przypadku przetwarzania w sposób inny niż zautomatyzowany, np. w formie tradycyjnej – papierowej, jeżeli dane stanowią lub mogą stanowić część zbioru[27].

Dane osobowe dzielą się na trzy kategorie:

[26] Tj. Dz. U. z 2018 r. poz. 1986 z późn. zm.

[27] W orzecznictwie Trybunału Sprawiedliwości UE pojęcie zbioru jest rozumiane szeroko - por. wyrok TSUE z 10 lipca 2018 r. w sprawie C-25/17, zgodnie z którym pojęcie „zbioru" obejmuje zestaw danych o ile dane te są zorganizowane wg określonych kryteriów umożliwiających w praktyce ich łatwe odnalezienie dla ich późniejszego wykorzystania. Jednocześnie nie jest konieczne aby taki zestaw zawierał kartoteki, szczególne rejestry lub inne systemy służące wyszukiwaniu.

1) **dane tzw. zwykłe**, takie jak imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail itp.;
2) szczególne kategorie danych osobowych (uprzednio zwane **danymi wrażliwymi**), wymienione w art. 9 RODO, tj. dane ujawniające:
   - pochodzenie rasowe lub etniczne,
   - poglądy polityczne,
   - przekonania religijne lub światopoglądowe,
   - przynależność do związków zawodowych,
   - dane genetyczne,
   - dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
   - dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
3) dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa wymienione w art. 10 RODO (uprzednio również zaliczane do **danych wrażliwych**).

Zasady przetwarzania danych osobowych ustanawia art. 5 RODO, ujmując je w formę podstawowych obowiązków administratora, zgodnie z którymi dane osobowe muszą być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**zgodność z prawem, rzetelność i przejrzystość**);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (**minimalizacja danych**);
- prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (**prawidłowość**);
- przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane (**ograniczenie przechowywania**);
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**integralność i poufność**).

Jednocześnie administrator jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie (**rozliczalność)**. Ta zasada kładzie nacisk na praktyczne aspekty wdrożenia RODO przez każdego administratora poprzez wprowadzenie w praktyce odpowiednich procedur i innych działań zapewniających przestrzeganie przepisów o ochronie danych osobowych.

Należy podkreślić, że RODO nie powstało w próżni normatywnej. 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 UE. Rozporządzenie 2016/679 opiera się na podstawowych wartościach istniejącego już systemu, utrzymując zasady ochrony danych oraz podstawy prawne przetwarzania danych, poddając je jedynie niezbędnym modyfikacjom.

RODO nakłada na administratorów obowiązek umożliwienia realizacji przez osoby, których dane dotyczą swoich praw. Do tych praw należą m.in.: prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych (tzw. prawo do bycia zapomnianym), prawo do ograniczenia przetwarzania, obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.

Istotnym uprawnieniem osoby, której dane dotyczą, jest wynikające z art. 15 RODO prawo dostępu do tych danych. Zgodnie ze wskazanym przepisem osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej

dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Równie istotnym uprawnieniem jest wskazane w art. 16 RODO prawo do sprostowania danych zgodnie z którym osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

2. Orzecznictwo sądów administracyjnych w sprawach decyzji lub postanowień organu nadzorczego

W 2018 r. wniesiono do Wojewódzkiego Sądu Administracyjnego w Warszawie[28] 77 skarg na decyzje lub postanowienia GIODO lub Prezesa UODO, co stanowi wzrost o 15 % w stosunku do roku 2017. W omawianym roku sprawozdawczym sądy administracyjne nie orzekały jednak merytorycznie w tych sprawach, natomiast wypowiedziały się co do wcześniejszych decyzji lub postanowień GIODO. WSA jedynie w 19 sprawach w całości lub w części negatywnie ocenił rozstrzygnięcia GIODO, natomiast w ponad 70 oddalił lub odrzucił skargi na decyzje lub postanowienia GIODO. Naczelny Sąd Administracyjny[29] jedynie w trzech sprawach oddalił skargi kasacyjne wniesione przez GIODO, a w 16 potwierdził stanowisko wyrażone w rozstrzygnięciach GIODO nie przychylając się do skarg kasacyjnych składanych przez pozostałe strony postępowania.

Należy również odnotować 24 decyzje stwierdzające bezczynność GIODO lub UODO, co wiązało się z szerszym problemem ograniczonych zasobów ludzkich Biura GIODO, umożliwiałyby który w pełni efektywne wykonywanie powierzonych mu zadań. Jak wcześniej wskazano znaczące zwiększenie zatrudnienia nastąpiło dopiero w drugiej połowie 2018 r.

[28] Dalej jako WSA
[29] Dalej jako NSA

3. Rozpatrywanie skarg

Postępowanie wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej dotyczące naruszenia przepisów o ochronie danych osobowych toczą się zgodnie z normami proceduralnymi określonymi przepisami ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[30]. W przypadku stwierdzenia naruszenia przepisów prawa, postępowanie to może zakończyć się wydaniem decyzji administracyjnej nakazującej administratorowi danych określone zachowanie lub nałożeniem administracyjnej kary pieniężnej. Pomimo autonomii proceduralnej państw członkowskich UE pewne kwestie proceduralne, zwłaszcza związane z postępowaniami transgranicznymi zostały bezpośrednio uregulowane w RODO. Niemniej w omawianym okresie sprawozdawczym Prezes UODO w dużej części zajmował się skargami, które wpłynęły przed 25 maja 2018 r., do których zastosowania znajdują dotychczasowe przepisy.

W omawianym okresie sprawozdawczym do organu nadzorczego wpłynęło 5565 skarg, z czego przeszło 4550 wpłynęło w okresie od 25 maja do 31 grudnia 2018 r. Należy jednocześnie zauważyć, że w dniu 25 maja 2018 r. przedmiotem postępowań przed Prezesem UODO było 4417 skarg, które wpłynęły przed tą datą, z czego od 1 stycznia 2018 r. wpłynęło jedynie 1330 skarg. Ze względu na dużą liczbę skarg wniesionych w poprzednim okresie sprawozdawczym, w 2018 r. przeważająca większość postępowań była prowadzona w związku ze skargami wniesionymi przed 25 maja 2018 r.

Postępowania administracyjne zainicjowane skargami indywidualnymi, wszczęte przez GIODO, a po 25 maja 2018 r. przez Prezesa UODO, dotyczące naruszenia przepisów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, a także przepisów RODO toczą się według przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[31]. Prezes UODO musiał za każdym razem ocenić, czy kwestionowany proces przetwarzania danych osobowych, do którego doszło w okresie obowiązywania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, był zgodny z prawem na dzień wydania decyzji administracyjnej, i czy był to proces zakończony lub też trwający dalej. Jeżeli był on zdarzeniem jednorazowym i dokonanym, do którego doszło w okresie obowiązywania ustawy z dnia 29 sierpnia 1997 r., do oceny zgodności z prawem tej okoliczności zastosowanie miały przepisy materialne tejże ustawy. W sytuacji, gdy dane osobowe były nadal przetwarzane, należało zastosować przepisy obowiązujące w czasie wydawania rozstrzygnięcia dla sprawy. Postępowania te kończą się wydaniem decyzji administracyjnej, mocą której Prezes UODO m.in.: umarza postepowanie, odmawia uwzględnienia wniosku skarżącego, nakazuje przywrócenie stanu zgodnego z prawem, nakłada karę, upomnienie albo ostrzeżenie na administratora czy podmiot przetwarzający. Ustawodawca krajowy wprowadził przy tym jednoinstancyjność postępowania, co znacząco przełożyło się na efektywność i terminowość załatwiania spraw przed Prezesem UODO.

GIODO, a po 25 maja 2018 r. Prezes UODO w roku 2018 rozstrzygał w sprawach dotyczących przetwarzania danych osobowych w kwestiach, które wielokrotnie były już przedmiotem postępowań

[30] tj. Dz. U. z 2018 r. poz. 2096 z późn. zm. – dalej jako: k.p.a.

w latach ubiegłych. Należy jednak wskazać, że zmiana stanu prawnego, do której doszło za sprawą rozporządzenia 2016/679, spowodowała zarówno znaczący wzrost liczby skarg, jak i konieczność stawienia czoła licznym nowym wyzwaniom po stronie administratorów oraz organu nadzoru. Administratorzy w toku prowadzonych postępowań zobowiązani są – zgodnie z zasadą rozliczalności – wykazać swoje przygotowanie i stosowanie nowych przepisów. Organ nadzorczy, z kolei, stale mierzy się z koniecznością dokonywania interpretacji nowych przepisów o ochronie danych osobowych. Skarżący oczekują przy tym od organu nie tylko badania legalności procesów przetwarzania ich danych, przetwarzania danych zgodnie z zasadami wykonywania operacji na danych, czy weryfikacji spełniania obowiązków informacyjnych z art. 13 i 14, ale także, (notabene często nie podejmując w pierwszej kolejności stosownych działań przed administratorem) chcą, aby organ nadzorczy wyręczył ich w realizacji ich praw z art. 15–22. Takie żądania skarżący składają zwłaszcza gdy kontakt z administratorem jest dla nich utrudniony.

Każda ze skarg analizowana jest na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami KPA oraz (w przypadku skarg, które wpłynęły do Biura GIODO przed 25 maja 2018 r.) wymogów fiskalnych wskazanych w ustawie o opłacie skarbowej[32]. W sytuacji gdy skarga nie spełnia warunków wymaganych przez ww. przepisy prawa, organ ochrony danych osobowych wzywa wnioskodawcę do uzupełnienia braków formalnych lub uiszczenia stosownej opłaty. W omawianym roku sprawozdawczym Prezes UODO wydawał postanowienia o zwrocie skargi na skutek nieuiszczenia opłaty skarbowej wyłącznie w zakresie spraw przejętych do prowadzenia od GIODO. Skargi składane do UODO od 25 maja 2018 r. nie podlegają bowiem opłacie skarbowej. Natomiast w sprawach, w których nie uzupełniono braków formalnych, skargi pozostawiano bez rozpoznania.

Kościoły i związki wyznaniowe

W omawianym roku sprawozdawczym wpływały skargi dotyczące przetwarzania danych osobowych przez proboszczów Kościoła katolickiego. Jednocześnie 13 marca 2018 r. został wydany przez Konferencję Episkopatu Polski Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim (Dekret), mocą którego został powołany Kościelny Inspektor Ochrony Danych[33]. Zgodnie z art. 35 ust. 1 Dekretu, Kościelny Inspektor Ochrony Danych jest niezależnym organem monitorującym i zapewniającym przestrzeganie przepisów o ochronie danych osobowych w ramach i zgodnie z działaniem Kościoła katolickiego i jego struktur. Kościelny Inspektor Ochrony Danych w zakresie wykonywania swoich zadań nadzorczych nie podlega poleceniom innych podmiotów. Zgodnie natomiast z art. 37 ust. 1 pkt 5 Dekretu, do zadań Kościelnego Inspektora Ochrony Danych należy rozpatrywanie skarg dotyczących przestrzegania przepisów ustanowionych w Kościele w zakresie ochrony danych osobowych. Dlatego też w takich sprawach Prezes Urzędu jest zobowiązany umorzyć postępowanie z uwagi na brak kompetencji w tym zakresie.[34]

W 2018 r. Prezes UODO rozpatrywał skargi[35] dotyczące niewykonania ciążącego na związku wyznaniowym – jako administratorze danych osobowych – obowiązku informacyjnego wynikającego z art. 15 RODO (prawo dostępu do danych). Prezes UODO w jednej ze spraw[36] ustalił, że związek wyznaniowy jest instytucją wpisaną do rejestru kościołów i innych związków wyznaniowych prowadzonych przez ministra właściwego do spraw wyznań religijnych i nie stosuje szczegółowych zasad ochrony osób fizycznych w związku z przetwarzaniem ich danych na podstawie art. 91 RODO,

[32] Ustawa z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz. U. z 2018 r. poz. 1044 z późn. zm.).

[33] Zob. art. 91 RODO.

[34] Decyzja z 19.10.2018 r. w sprawie ZSPU.440.585.2018

[35] np. ZSPU.440.99.2018; ZSPU.440.279.2018

[36] ZSPU.440.99.2018

w związku z tym Prezes UODO uznał, że jest właściwym organem nadzorczym do rozpoznania skargi dotyczącej działań tego związku.

Zdaniem organu ochrony danych osobowych wniosek o spełnienie prawa dostępu do danych został złożony poprawnie. Prezes UODO stwierdził, że obowiązek informacyjny, o którym jest mowa w art. 15 RODO (dawniej art. 33 w zw. z art. 32 ust. 1 pkt 1-5a ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych z 1997 r.) wobec byłych członków związku nie został spełniony i wydał decyzję[37] nakazującą związkowi wyznaniowemu jego spełnienie w zakresie żądanym przez wnioskodawców.

Bezpieczeństwo obiegu dokumentów w Miejskim Ośrodku Pomocy Społecznej

W 2018 r. do organu ochrony danych osobowych wpłynęła skarga[38] na pozyskanie danych osobowych przez pracownika Miejskiego Ośrodka Pomocy Społecznej (MOPS) za pomocą telefonu komórkowego. W trakcie wywiadu środowiskowego (przeprowadzanego w związku z wnioskiem o przyznanie pomocy w formie usług opiekuńczych) w miejscu zamieszkania Skarżącej, pracownik MOPS wykonał telefonem zdjęcia decyzji emerytalnych skarżącej wydanych przez Zakład Ubezpieczeń Społecznych.

Prezes UODO mając na uwadze definicję dokumentu elektronicznego (art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[39]) stwierdził, że telefon komórkowy posiadający pamięć lub zaopatrzony w jej nośnik jest urządzeniem, które może służyć do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej.[40] Z uwagi na wątpliwości, co do tego, czy MOPS posiada sformalizowane procedury dotyczące obiegu dokumentów w wersji elektronicznej, na podstawie art. 52 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Prezes UODO skierował wystąpienie do MOPS zmierzające do zapewnienia skutecznej ochrony danych osobowych[41]. Podkreślił, że administrator danych osobowych ma zarówno obowiązek zorganizowania bezpieczeństwa procesu przetwarzania danych osobowych, w sposób odpowiadający przepisom obowiązującym w zakresie przetwarzania danych osobowych, jak i prawo dokonania tego w taki sposób, który odpowiadał będzie zagrożeniom oraz kategoriom przetwarzania danych. Administrator danych osobowych decyduje i odpowiada za przetwarzanie danych zgodnie z prawem. Organ ochrony danych osobowych zaakcentował, że przetwarzając dane osobowe należy brać pod uwagę odpowiedzialność, zarówno cywilną, jak i karną.

Powierzanie przetwarzania danych osobowych

Prezes UODO prowadził w 2018 r. postępowania, w których administrator danych osobowych udostępnił dane osobowe na podstawie zawartej umowy powierzenia. W jednej ze spraw burmistrz działający w imieniu gminy zawarł umowę powierzenia przetwarzania danych osobowych radnych spółce w celu realizacji umowy dotyczącej pomocy w obsłudze informatycznej sesji Rady Gminy. Skarżący zarzucił, że Sekretarz Gminy bezprawnie udostępnił spółce jego dane osobowe w postaci prywatnego numeru telefonu komórkowego i prywatnego adresu e-mail w związku z pełnieniem przez skarżącego funkcji publicznej – radnego Rady Miejskiej.

Prezes UODO stwierdził[42], że gmina wykonuje ustawowe zadania m.in. poprzez działalność swoich organów, tj. rady miejskiej i burmistrza. Przytoczył art. 28 i art. 32 RODO, z analizy których wynika, że powierzenie przez burmistrza danych osobowych radnych spółce w celu realizacji umowy dotyczącej pomocy w obsłudze informatycznej sesji rady gminy i w zakresie niezbędnym do prawidłowego jej wykonania, odbyło się zgodnie z prawem. Należy podkreślić, że przetwarzanie

[37] decyzja z 20.12.2018 r. w sprawie ZSPU.440.99.2018
[38] ZSPU.440.192.2018
[39] Tj. Dz. U. z 2019 poz. 700 z późn. zm.
[40] decyzja z 30.11.2018 r. w sprawie ZSPU.440.192.2018
[41] wystąpienie z 30.11.2018 r. w sprawie ZSPU.440.192.2018
[42] decyzja z 30.11.2018 r. w sprawie ZSPU.440.100.2018;

przez burmistrza i spółkę danych osobowych w postaci numeru telefonu komórkowego oraz adresu e-mail skarżącego w związku z pełnieniem przez niego funkcji publicznej radnego było uzasadnione w świetle art. 6 ust. 1 lit c) i e) RODO z uwagi na wypełnianie obowiązku prawnego ciążącego na administratorze oraz wykonywanie zadania realizowanego w interesie publicznym i w ramach sprawowania władzy publicznej.

Przetwarzanie danych osobowych przez burmistrzów dzielnic m. st. Warszawy

W 2018 r. należy odnotować często pojawiające się wątpliwości dotyczące statusu burmistrzów poszczególnych dzielnic m. st. Warszawy. W jednej ze spraw skarżący zakwestionował udostępnienie jego danych osobowych dotyczących udziału w konkursie na dyrektora jednej ze szkół wszystkim burmistrzom m. st. Warszawy. W wydanej w tej sprawie decyzji GIODO wskazał[43], że administratorem danych osobowych przetwarzanych przez burmistrzów poszczególnych dzielnic jest Prezydent m.st. Warszawy, a nie poszczególni burmistrzowie. To Prezydent jest organem wykonawczym samorządu terytorialnego, decydującym o celach i środkach przetwarzania danych osobowych. Jednocześnie dzielnica – w myśl przepisów ustawy o ustroju m.st. Warszawy – jest jednostką pomocniczą m.st. Warszawy, działającym w oparciu o statut nadany przez Radę m.st. Warszawy. Tym samym burmistrz dzielnicy nie jest odrębnym administratorem danych osobowych. Rozstrzygnięcie to rozwiało wątpliwości w tym zakresie.

GIODO – odnosząc się do kwestii rozesłania przez burmistrza dzielnicy do burmistrzów innych dzielnic m.st. Warszawy, pisma zawierającego takie dane jak m.in.: imię, nazwisko, adres zamieszkania i informacje dotyczące wykształcenia skarżącego - wskazał, że działanie to było nieprawidłowe. Stosownie bowiem do treści art. 26 ust. 1 pkt 3 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (aktualnie art. 5 ust. 1 lit. b) RODO), administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (tzw. zasada celowości). W niniejszej sprawie, zasada ta została naruszona. Jednocześnie należy zwrócić uwagę, że w wyniku przedmiotowego działania burmistrza dzielnicy, dane osobowe skarżącego zostały co prawda błędnie przekazane burmistrzom innych dzielnic m.st. Warszawy, niemniej przekazanie to odbyło się w ramach działalności jednego administratora, tj. Prezydenta.

Zamieszczanie numeru PESEL w decyzji administracyjnej

W 2018 r. należy także odnotować skargi dotyczące prawidłowości zamieszczania numerów PESEL przy oznaczaniu stron postępowania w decyzji administracyjnej. Uznano, że takie oznaczanie nie jest prawidłowe. Zgodnie z art. 107 § 1 k.p.a. elementem obligatoryjnym decyzji administracyjnej jest m.in. oznaczenie strony lub stron postępowania (pkt 3). Prezes UODO wskazał w decyzji[44], że z powołanego przepisu nie wynika, aby do oznaczenia strony postępowania niezbędne było podanie numeru PESEL. W opinii organu ds. ochrony danych osobowych, w przypadku osób fizycznych będących stroną postępowania administracyjnego wystarczające jest podanie takich danych, jak: imię, nazwisko oraz adres zamieszkania. Inne dane mogą być podawane tylko wówczas, gdy wynika to wprost z przepisu prawa, np. art. 126 § 2 pkt 2 k.p.c.

Jednocześnie Prezes UODO wskazywał[45], że oznaczanie stron postępowania powinno odbywać się zgodnie z zasadą minimalizacji przewidzianą w art. 5 ust. 1 lit. c) RODO, zgodnie z którą

[43] decyzja z 12.01.2018 r. w sprawie DOLiS-440-1534/17;

[44] decyzja z 11.10.2018 r. w sprawie ZSPU.440.379.2018; decyzja z 25.10.2018 r. w sprawie ZSPU.440.535.2018;

[45] wystąpienie z 22.10.2018 r. w sprawie ZSPU.440.379.2018; wystąpienie z 25.10.2018 r. w sprawie ZSPU.440.535.2018;

dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane, a administrator jest odpowiedzialny za przestrzeganie ww. przepisu i musi być w stanie wykazać jego przestrzeganie zgodnie z zasadą rozliczalności (ust. 2). Zasada ta wprowadza ilościowe ograniczenie zbierania i dalszego przetwarzania danych osobowych, w myśl której dane muszą być odpowiednie i stosowne do osiągnięcia celu ich zebrania, ale jednocześnie nie mogą być nadmierne w stosunku do zamierzonego celu. Tym samym przetwarzanie danych w zakresie zbędnym oznacza naruszenie przepisów o ochronie danych osobowych. Z tego względu przetwarzanie danych, które potencjalnie w przyszłości mogą być użyteczne (argument taki wskazywali administratorzy danych osobowych), nie jest dopuszczalne.

W ocenie Prezesa UODO nie ma podstaw prawnych, aby strony postępowania były oznaczone za pomocą numeru PESEL. Oznaczenie strony lub stron w decyzji administracyjnej powinno zawierać tylko te dane, które są niezbędne do wypełnienia obowiązku wynikającego z art. 107 § 1 Kpa, a więc do osiągnięcia celu jakim jest wydanie decyzji administracyjnej. Oznaczenie strony w celu wydania decyzji administracyjnej z podaniem jej numeru PESEL jest niecelowe, zbędne dla realizacji pierwotnego celu przetwarzania, nie uzasadnia podania innych danych służących oznaczeniu strony niż imię, nazwisko i miejsce zamieszkania.[46]
Jednak, co Prezes UODO podkreślał w wielu decyzjach[47] – nie może on ingerować w treść wydanej przez inny organ decyzji administracyjnej, a co za tym idzie – mimo stwierdzonego naruszenia – nie może nakazać usunięcia z decyzji numeru PESEL ze względu na brak właściwości i kompetencji w tym zakresie.

Udostępnianie danych osobowych w Biuletynie Informacji Publicznej
W omawianym okresie sprawozdawczym przeważająca część dotyczących podmiotów publicznych skarg odnosiła się do przetwarzania danych osobowych w Biuletynie Informacji Publicznej[48]. Ustawodawca w art. 4 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[49] zobowiązuje podmioty publiczne i inne wykonujące zadania publiczne do udostępniania informacji publicznej w BIP[50]. Ograniczenia[51] prawa do przedmiotowej publikacji wynikają z przepisów o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, a także ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy[52]. Nie dotyczy to 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.

Dokonując analizy ciążącego na administratorze obowiązku, aby przetwarzane przez niego dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami[53] (zasada ograniczenia celu[54]), Prezes UODO stoi na stanowisku, że zbierane dane muszą były adekwatne do celów, w jakich są

[46] Zob. także https://uodo.gov.pl/pl/138/561;
[47] np. decyzja z 11.10.2018 r. w sprawie ZSPU.440.379.2018; decyzja z 25.10.2018 r. w sprawie ZSPU.440.535.2018;
[48] Dalej jako: BIP
[49] Tj. Dz. U. z 2019 r., poz. 1429 - dalej jako: u.d.i.p.
[50] Zob. art. 7 ust. 1 pkt 1 u.d.i.p;
[51] Zob. art. 5 ust. 1 u.d.i.p.;
[52] Zob. art. 5 ust. 2 u.d.i.p.;
[53] dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami;
[54] Wskazana w art. 5 ust. 1 lit. b) RODO;

przetwarzane. Jednocześnie rodzajem i treścią dane nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania. Omawiany wymóg sprzeciwia się też zbieraniu zarówno wszelkich danych dla tego celu nieistotnych, niemających znaczenia, jak i danych o „większym - niż uzasadniony z tego względu - stopniu szczegółowości". Przy tym administrator jest każdorazowo zobowiązany do ustalenia zależności między celem a zakresem przetwarzania danych oraz powinien ograniczyć przetwarzanie danych jedynie do tych, które są niezbędne do osiągnięcia celu (zasada minimalizacji danych[55]).

W jednej ze spraw na stronie BIP opublikowano treść wystąpienia pokontrolnego, udostępniając tym samym dane osobowe skarżącego, w zakresie pełnionej przez niego funkcji w spółce, okresie jej pełnienia oraz wysokości otrzymanego przez niego wynagrodzenia. W ocenie Prezesa UODO[56] wskazanie w ww. wystąpieniu pokontrolnym na zajmowane przez skarżącego stanowisko w spółce wraz z jego inicjałami, z uwagi, iż stanowisko to było jednoosobowe, pozwala na jednoznaczne jego zidentyfikowanie. Jednocześnie podkreślił, że skarżący otrzymując wynagrodzenie za swoją pracę w związku z zawartą z nim umową cywilnoprawną nie był ani funkcjonariuszem publicznym, ani osobą pełniąca taką funkcję. Umieszczanie informacji w zakresie wysokości wynagrodzenia w wystąpieniu pokontrolnym udostępnionym dla szerokiego kręgu odbiorców, tj. na stronie internetowej BIP, stanowi w ocenie GIODO naruszenie prawa do prywatności.[57]

W sprawach prowadzonych w 2018 r. często pojawiającą się wątpliwością była kwestia czasowego ograniczenia przetwarzania danych osobowych[58] (zasada ograniczenia przechowywania). Przepisy nie precyzują okresu udostępniania informacji w BIP (ani minimalnego, ani maksymalnego). W ocenie Prezesa UODO[59], nie oznacza to jednak, że informacje te mogą być udostępniane bezterminowo. Zdaniem organu ochrony danych osobowych należy stosować w tej kwestii zasadę ograniczenia przetwarzania. Dlatego administrator danych powinien regularnie dokonywać przeglądu swych zbiorów pod kątem usuwania zbędnych danych.[60]

Częstym przedmiotem skarg było także upublicznianie w BIP treści uchwał organów administracji bez stosownej anonimizacji. W jednej z decyzji[61] Prezes UODO stwierdził, że udostępnianie w BIP uchwał organów gminy zawierających niezanonimizowane dane osobowe osób uczestniczących w posiedzeniach narusza przepisy o ochronie danych osobowych. Udostępnienie takie

[55] art. 5 ust. 1 lit. c) RODO;

[56] decyzja z 30.11.2018 r. w sprawie ZSPU.440.456.2018;

[57] zob. także decyzja z 27.02.2018 r. w sprawie DOLiS-440-922/15; por. wyrok NSA z 30 września 2015 r., sygn. akt I OSK 1853/14, w którym wskazano, że cyt.: (…) rozważając możliwość udostępnienia informacji o wynagrodzeniu danej osoby organ powinien każdorazowo analizować, czy jest ona niezbędna z punktu widzenia celów prawa do informacji publicznej, a także czy nie narusza godności i intymności osoby, której taka informacja dotyczy (…)";

[58] Zgodnie z art. 5 ust.1 lit. e) RODO dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

[59] pismo z 16.11.2018 r. w sprawie ZSPU.027.42.2018;

[60] zob. wyrok Wojewódzkiego Sądu Administracyjnego w Lublinie z 1 marca 2016 r. (sygn. akt II SA/Lu 876/15);

[61] decyzja z 20.11.2018 r. w sprawie ZSPU.440.523.2018;

nie spełnienia bowiem żadnej z przesłanek legalności przetwarzania danych osobowych, określonych w art. 6 ust. 1 lit. a) – f) RODO.[62]

Podobnie jak w latach poprzednich Prezes UODO wskazuje, że administratorzy danych osobowych z sektora publicznego niestarannie podchodzą do wymogów dotyczących anonimizowania dokumentów publikowanych w BIP, usuwając dane osobowe w nich zawarte dopiero po uzyskaniu informacji o wpłynięciu skargi do organu ochrony danych osobowych.[63] Zdarzają się też sytuacje, że mimo usunięcia przez administratora dokumentu zawierającego dane osobowe z BIP, przedmiotowy dokument ten nadal jest dostępny w wersji historycznej.[64] Prezes Urzędu stoi na stanowisku, że publikowane i przekazywane dane osobowe powinny być dokładnie sprawdzane przez zobowiązane organy, w celu uniknięcia pomyłek i sytuacji grożących naruszeniem dóbr osobistych w związku z nieprzestrzeganiem przepisów z zakresu ochrony danych osobowych.[65]

W jednej ze spraw burmistrz opublikował oświadczenie majątkowe skarżącego wraz z załączonymi zeznaniami podatkowymi PIT-11 i PIT-37, ujawniając tym samym dane osobowe skarżącego i jego żony w zakresie imienia i nazwiska, adresu zamieszkania, numeru pesel oraz wysokości dochodów. Korzystając z uprawnienia zawartego w art. 58 ust. 2 lit. b) RODO, Prezes wystosował upomnienie[66] do burmistrza, wskazując że publikowane i przekazywane dane osobowe powinny być dokładnie sprawdzane, aby uniknąć pomyłek i sytuacji grożących naruszeniem dóbr osobistych. Ich źródłem w prawie polskim jest Konstytucja i podlegają ochronie zarówno cywilnoprawnej jak i karnoprawnej. Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest także jednym z praw podstawowych, zawartych w Karcie praw podstawowych Unii Europejskiej[67]. Przetwarzanie danych osobowych nie może naruszać podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludziom, tj. tak żeby obywatele mieli dostęp do informacji na temat majątku radnych bez jednoczesnego naruszania dóbr osobistych tych ostatnich. W przedmiotowej sprawie[68] Prezes Urzędu skierował także do właściwej prokuratury zawiadomienie o podejrzeniu popełnienia przestępstwa.[69]

Podsumowując, należy wskazać, że administrator danych osobowych nie może zakładać automatyzmu przy publikacji danych osobowych na stronach BIP, tj. upublicznienia wszelkich danych osobowych i ich dalszego nieograniczonego w czasie przetwarzania. Administrator jest zobowiązany, do każdorazowego dokonania stosownej oceny tak zasadności upublicznienia danych osobowych konkretnej osoby, jak i określenia końca ich dalszej retencji.

[62] zob. także decyzja z 19.09.2018 r. w sprawie ZSPU.440.30.2018; decyzja z 23.10.2018 r. w sprawie ZSPU.440.146.2018; decyzja z 07.12.2018 r. w sprawie ZSPU.440.603.2018; decyzja z 13.12.2018 r. w sprawie ZSPU.440.560.2018; decyzja z 23.05.2018 r. w sprawie ZSPU.440.343.2018;

[63] zob. np. decyzja z 05.11.2018 r. w sprawie ZSPU.440.92.2018, decyzja z 24.07.2018 r. w sprawie ZSPU.440.21.2018, decyzja z 15.11.2018 r. w sprawie ZSPU.440.519.2018, decyzja z 15.11.2018 r. w sprawie ZSPU.440.1239.2018; decyzja z 07.03.2018 r. w sprawie DOLiS-440-1075/17; decyzja z 15.11.2018 r. w sprawie ZSPU.440.519.2018; decyzja z 15.11.2018 r. w sprawie ZSPU.440.271.2018;

[64] ZSPU.440.163.2018

[65] decyzja z 06.12.2018 r. w sprawie ZSPU.440.46.2018;

[66] decyzja z 06.12.2018 r. w sprawie ZSPU.440.46.2018;

[67] Karta praw podstawowych Unii Europejskiej (Dz.U.UE z C z dnia 14.12,2007 r.) (2007/C 303/01);

[68] ZSPU.440.46.2018;

[69] zawiadomienie o podejrzeniu popełnienia przestępstwa z 06.12.2018 r. w sprawie ZSPU.440.46.2018;

Ochrona danych osobowych osób zawiadamiających o nieprawidłowościach

W 2018 r. wpływały także skargi[70] od osób, które sygnalizowały organom publicznym działania niezgodne z prawem innych podmiotów.

W jednej ze spraw[71] burmistrz przeprowadził wobec właściciela sąsiedniej działki postępowanie kontrolne na skutek sygnału skarżącej zawartego w ww. piśmie skierowanym do burmistrza. Skarżąca w odpowiedzi na swój sygnał otrzymała pismo informujące ją, iż kopia jej pisma adresowanego do burmistrza została przekazana właścicielowi działki. W ocenie Prezesa UODO przedmiotowe udostępnienie danych naruszyło art. 5 ust. 1 lit. a) i b) RODO, jak również art. 6 ust. 1 RODO. Niedopuszczalne było bowiem udostępnienie danych osobowych skarżącej na rzecz właściciela sąsiedniej działki, gdyż postępowanie wobec tej osoby prowadzone było na podstawie odrębnych przepisów ustawy o utrzymaniu porządku i czystości w gminach[72] i jego stroną był wyłącznie właściciel sąsiedniej działki jako podmiot kontrolowany.

W opisywanej sprawie Prezes Urzędu wystosował do burmistrza wystąpienie[73], wskazując na potrzebę wyeliminowania praktyk polegających na niezasadnym udostępnianiu danych osobowych tzw. sygnalistów, czyli osób zgłaszających nieprawidłowości w sprawach, w których nie są stroną (ani uczestnikiem), na rzecz stron (uczestników) tych postępowań. Prezes podkreślił, że niezbędne jest zapewnienie ochrony danych osobowych sygnalistów, którą umożliwia stosowanie zarówno przepisów k.p.a., dotyczących procedury rozpatrywania skarg i wniosków, jak również RODO. W ocenie organu dane osobowe osób wnoszących taką skargę (sygnalistów) nie podlegają ujawnieniu w toku ww. postępowania. Co więcej, nie mają żadnego znaczenia dla takiego postępowania, którego celem jest zweryfikowanie i wyeliminowanie sygnalizowanych nieprawidłowości. Nawet jeżeli na skutek tych skarg zostaną wszczęte odrębne postępowania, przewidziane przepisami szczególnymi. Osoby te w żadnym razie nie stają się ich stronami w rozumieniu art. 28 k.p.a. Pozostają one nadal wyłącznie osobami sygnalizującymi swoje niezadowolenie z nienależytego wykonywania zadań przez właściwe organy, oczekującymi na zawiadomienie ich o reakcji na sygnalizowany problem. Tym samym dane takich osób powinny podlegać ochronie szczególnej z uwagi na możliwe konsekwencje w sferze naruszenia ich interesów przez faktyczne strony postępowań zainicjowanych na skutek ich sygnału. Zdaniem Prezesa Urzędu sprawy dotyczące sygnałów osób powinny być prowadzone odrębnie (z odrębną sygnaturą), a o efektach działań podjętych na skutek ich interwencji (sygnału) powinny być one informowane w osobnym piśmie. Sygnaliści nie mają też statusu świadków.

Ponadto Prezes Urzędu wskazał, że udostępnienie danych osobowych sygnalistów narusza zasadę celowości. Ustalając cel, administrator powinien odwołać się do okoliczności sprawy i powodu, dla którego te dane zostały zebrane oraz każdorazowo dokonać starannej analizy zasadności udostępnienia danych.

Generalny Inspektor w innym wystąpieniu[74] w analogicznej sprawie wskazał, że osoby informujące o patologiach pełnią niezastąpioną funkcję w społeczeństwie. Dlatego tak ważne jest stworzenie mechanizmów pozwalających ograniczyć osobiste ryzyko ponoszone przez jednostki alarmujące o nieprawidłowościach, tak aby posiadając wiedzę na określony temat nie bały się jej ujawniać właściwym organom. Wpłynie to pozytywnie na poziom bezpieczeństwa całego społeczeństwa.

Tożsamy pogląd Prezes UODO wyraził w decyzji[75] wydanej w sprawie, w której skarżący wraz z innymi mieszkańcami wsi (łącznie aż 121 osób) złożył w urzędzie gminy wniosek o odwołanie sołtysa. Wniosek ten zawierał takie dane osobowe wnioskodawców, jak: imię, nazwisko, podpis, adres,

[70] zob. np.: ZSPU.440.214.2018; decyzja z 26.02.2018 r. w sprawie DOLiS-440-1274/14;
[71] ZSPU.440.214.2018;
[72] ustawa z dnia 13.09.1996 r. ustawy o utrzymaniu porządku i czystości w gminach (Dz. U. z 2018 r., poz. 1454);
[73] wystąpienie w sprawie ZSPU.440.214.2018;
[74] wystąpienie z 01.03.2018 r. w sprawie DOLiS-440-1753/15.
[75] decyzja z 08.11.2018 r. w sprawie ZSPU.440.159.2018;

nr PESEL. Sołtys zwrócił się do urzędu gminy o wgląd do akt sprawy dotyczących odwołania z pełnionej funkcji. Udostępniony wniosek o odwołanie sołtysa został zanonimizowany w zakresie numeru PESEL oraz podpisu wnioskujących, zawierał natomiast ich imiona, nazwiska oraz miejsce zamieszkania (nazwę miejscowości).

Prezes UODO w wydanej w tej sprawie decyzji wskazał, że wniosek sołtysa nie mógł być rozpatrywany w trybie dostępu do informacji publicznej (na co wskazywał wójt), zatem podstawy prawnej do udostępnienia danych zawartych we wniosku nie mógł stanowić art. 23 ust. 1 pkt 2 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (obecnie art. 6 ust. 1 lit. c) RODO), który miałby odniesienie w zakresie do ustawy o dostępie do informacji publicznej. Co więcej, przepis ten nie mógł mieć również zastosowania do przepisów k.p.a, gdyż sołtys wsi nie mógł korzystać z uprawnienia przysługującego stronie postępowania administracyjnego w trybie art. 73 k.p.a[76].

Udostępnianie danych osobowych osób nie będących stroną postępowania administracyjnego

W 2018 r. wpływały również skargi dotyczące prawidłowości udostępniania danych osobowych stronom postępowania, w sytuacji gdy podmiot danych nie był stroną postępowania, ani nawet nie sygnalizował nieprawidłowości w działaniach innych podmiotów.

W jednej ze spraw skarżący zwrócił się do powiatowego inspektora nadzoru budowlanego (PINB) (za pośrednictwem urzędu gminy) z wnioskiem o przedstawienie prawnych uwarunkowań dla realizacji obiektów budowlanych, wskazując jednocześnie przykładowe numery działek. Na skutek powyższego PINB podjął działania wyjaśniające wobec właścicieli działek, które jako przykład skarżący podał we wniosku. Oryginał wniosku został dołączony do akt spraw wyjaśniających wraz z dokładnymi danymi osobowymi skarżącego i udostępniony do wglądu właścicielom działek, wobec których PINB wszczął postępowanie. Skarżący podniósł, że w konsekwencji właściciele działek kontaktowali się z nim bezpośrednio, powołując się na dane udostępnione w urzędzie, a niektóre ustne wypowiedzi można było zinterpretować jako pogróżki.

W wydanej w tej sprawie decyzji[77] GIODO wskazał, że PINB wszczynając postępowania z urzędu, powinien był uwzględnić wynikające z ustawy o ochronie danych osobowych zasady przetwarzania danych osobowych skarżącego. PINB – jako administrator danych osobowych – jest zobowiązany do dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnienia, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Niewątpliwie PINB jako podmiot właściwy do rozpatrzenia wniosku o przedstawienie prawnych uwarunkowań dla realizacji obiektów budowlanych, ma prawo przetwarzać dane osobowe skarżącego, jako osoby wnioskującej, jednak w ocenie GIODO, niewłaściwe jest ich dalsze udostępnienie podmiotom, wobec których organ wszczyna postępowania kontrolne związane z realizacją robót budowlanych na wskazanych przez skarżącego we wniosku działkach. Skarżący nie otrzymał w tych postępowaniach statusu strony, tym samym nie dotyczyły one jego interesu prawnego bądź obowiązku. Dlatego też wniosek skarżącego, wraz z jego danymi, nie powinien zostać przez PINB włączony do akt ww. postępowań, jedynie zainicjowanych tym wnioskiem, ale wszczętych z urzędu.

GIODO wskazał, że takie praktyki są nieprawidłowe, bowiem administrator danych osobowych nie wziął pod uwagę prawa do prywatności wnioskodawcy. Udostępnienie danych osobowych zawartych we wniosku stronom wszczętych postępowań jest nieadekwatne do celu ich pozyskania. Bezsporne jest zatem, iż w następstwie takich działań dochodzi do udostępnienia danych osobowych podmiotom do tego nieuprawnionym (stronom wszczętych postepowań).[78]

[76] zgodnie z którym strona ma prawo wglądu w akta sprawy, sporządzania z nich notatek, kopii lub odpisów, ponieważ w niniejszej sprawie nie było prowadzone postępowanie administracyjne, którego byłby stroną;
[77] decyzja z 28.02.2018 r. w sprawie DOLiS-440-461/17;
[78] zob. także wystąpienie z 22.11.2018 r. w sprawie ZSPU.440.260.2018;

Przetwarzanie danych w ramach procedury „Niebieskiej Karty"

W omawianych roku sprawozdawczym wpływały także skargi[79] dotyczące przetwarzania danych osobowych w związku z wszczęciem procedury „Niebieskiej Karty". Następuje ono w przypadku powzięcia podejrzenia stosowania przemocy wobec członków rodziny lub w wyniku zgłoszenia dokonanego przez członka rodziny. W treści skarg zarzucono pracownikom organów odpowiedzialnych za procedurę m.in. złamanie tajemnicy zawodowej oraz nieprawidłowości ich działań, a także podważano prawdziwość zebranych dowodów. Jednak organ ds. ochrony danych nie jest właściwy do wyznaczania granic tajemnicy zawodowej oraz stwierdzania jej naruszenia.

Właściwy do zbadania zakresu tajemnicy zawodowej oraz ewentualnego jej przekroczenia jest sąd powszechny. Jak wskazał w wyroku WSA w Warszawie[80] prawodawca określił uczestników procedury Niebieskiej Karty jako osobę, co do której istnieje podejrzenie, że jest dotknięta przemocą w rodzinie lub osobę, co do której istnieje podejrzenie, że stosuje przemoc w rodzinie. Sąd podkreślił, że organ ochrony danych osobowych nie może ingerować w stan faktyczny ustalony przez inne organy, ani nie może nadzorować prawidłowości i prawdziwości zgromadzonego materiału dowodowego w ramach tej procedury.

W decyzjach[81] Prezesa UODO wskazywano także, że ramach procedury „Niebieskiej Karty" zgodnie z art. 9a ustawy o przeciwdziałaniu przemocy w rodzinie tworzy się zespół interdyscyplinarny. Ww. przepis wymienia przedstawicieli jednostek wchodzących w jego skład. Ponadto w ramach powołanego zespołu interdyscyplinarnego, zgodnie z art. 9a ust. 10 ustawy mogą być tworzone grupy robocze, które mają na celu rozwiązywanie problemów związanych z wystąpieniem przemocy w rodzinie w indywidualnych przypadkach. W ich skład, zgodnie z art. 9a ust. 11 ustawy wchodzą przedstawiciele: 1) jednostek organizacyjnych pomocy społecznej; 2) gminnej komisji rozwiązywania problemów alkoholowych; 3) Policji; 4) oświaty; 5) ochrony zdrowia. Zdaniem Prezesa UODO organ publiczny odpowiedzialny za procedurę Niebieskiej Karty zgodnie z ww. przepisem ma obowiązek w ramach powołanej grupy roboczej poinformować np. pedagoga szkolnego czy dzielnicowego o spotkaniu, albowiem obecność przedstawiciela służb współpracujących z rodziną ma na celu zarówno opracowanie i realizację planu pomocy (art. 9b ust. 3 pkt. 1), jak i monitorowanie sytuacji w niej występującej (art. 9b ust. 3 pkt. 2). Organ publiczny wypełnia tym samym ciążący na administratorze obowiązek przetwarzania danych osobowych w myśl art. 6 ust. 1 lit. c) RODO.

Prezes UODO stoi na stanowisku, że przewidziana w art. 9c ust. 1 ustawy o przeciwdziałaniu przemocy w rodzinie możliwość przetwarzania danych osób dotkniętych przemocą w rodzinie i osób stosujących przemoc w rodzinie bez zgody i wiedzy tych osób jest jednym z narzędzi zapewniających koordynację oraz realizację stosownych działań podejmowanych przez zespół interdyscyplinarny oraz tworzone przez niego grupy robocze.

Przetwarzanie danych osobowych dłużnika

W 2018 r. utrzymał się trend składania skarg na przetwarzanie danych osobowych związane z dochodzeniem roszczeń od dłużników. W postępowaniach przed organem dłużnicy kwestionowali zasadność roszczenia, a czasem również wskazywali na brak ich zgody na przetwarzanie danych osobowych przez wierzyciela. W konsekwencji rozstrzygnięcia wydawane przez organ w zasadniczej większości przypadków sprowadzały się do odmowy uwzględnienia wniosków skarżących, np. o stwierdzenie braku podstawy do przetwarzania danych oraz opierały się o następującą

[79] np. ZSPU.440.388.2018;

[80] wyrok WSA w Warszawie z 22.11.2018 r. sygn. akt II SA/Wa 1875/17;

[81] decyzja z 07.11.2018 r. w sprawie ZSPU.440.63.2018; decyzja z 16.01.2018 r. w sprawie DOLiS-440-754/14; decyzja z 12.12.2018 r. w sprawie ZSPU.440.232.2018;

argumentację: podmioty z sektora prywatnego przetwarzają dane osobowe w celu dochodzenia roszczeń przysługujących im w stosunku do osób fizycznych praktycznie bezterminowo.

Zgodnie z przepisami Kodeksu cywilnego[82] zobowiązanie, po jego przedawnieniu, staje się zobowiązaniem naturalnym, tj. takim, którego wierzyciel nie może zaspokoić w ramach egzekucji, w przypadku podniesienia przez dłużnika zarzutu przedawnienia w postępowaniu przed sądem powszechnym. Zarówno przed podniesieniem ww. zarzutu w toku postępowania sądowego, jak i po wydaniu prawomocnego orzeczenia przez sąd powszechny o oddaleniu powództwa z uwagi na przedawnienie roszczenia, administrator będący wierzycielem jest uprawniony do przetwarzania danych osobowych skarżącego w celu dochodzenia roszczeń środkami pozasądowymi, np. wielokrotnymi wezwaniami do zapłaty, co, jak można wywnioskować ze skarg rozpatrywanych przez organ w 2018 r., jest dla skarżących uciążliwe.

W 2018 r. organ ochrony danych osobowych wielokrotnie wydawał decyzje w sprawach, w których sąd powszechny oddalił powództwo z uwagi na przedawnienie roszczenia, jednakże w dalszym ciągu administrator był uprawniony do przetwarzania danych osobowych dłużnika na podstawie prawnie usprawiedliwionego celu administratora danych osobowych, to jest w celu dochodzenia tego roszczenia.

Z uwagi na to, że administrator był uprawniony do przetwarzania danych osobowych, jeżeli spełnił przynajmniej jedną z przesłanek określonych w art. 23 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, a obecnie w art. 6 RODO. Przy czym w takich sytuacjach nie było i nie jest konieczne uzyskiwanie przez wierzyciela zgody dłużnika na przetwarzanie jego danych osobowych.

GIODO, a obecnie Prezes UODO, nie ma kompetencji do oceny, czy zobowiązanie istnieje oraz czy dochodzenie go w określonej wysokości przez wierzyciela jest zasadne, dopóki kwestii istnienia lub nieistnienia zobowiązania w stosunku do osoby fizycznej nie rozstrzygnie sąd powszechny. Wierzyciel ma prawo dochodzić swoich roszczeń również środkami pozasądowymi, zatem nie jest konieczne, by legitymował się tytułem wykonawczym w stosunku do dłużnika, chcąc dochodzić od niego roszczenia.

Oczywiście w wielu z rozstrzyganych sprawach organ ochrony danych osobowych badał także to, czy wierzyciel przetwarzając dane osobowe dłużnika, powinien czynić na nich operacje wyłącznie w zakresie koniecznym do dochodzenia roszczenia, tj. w zakresie adekwatnym do tego celu.

Wnioski o udostępnienie danych osobowych

Jedną z istotnych kwestii rozstrzyganych w sprawach prowadzonych zarówno przed GIODO, jak i Prezesem UODO w 2018 r. była zasadność żądania udostępnienia danych osobowych skarżącym dla zrealizowania różnego rodzaju celów. Najczęściej wskazywanym celem była konieczność pozyskania danych w celu wytoczenia powództwa przeciwko osobie, której dane dotyczą, np. w celu ochrony dóbr osobistych[83].

Zadaniem organu było ustalenie, czy administrator ustosunkował się do całego żądania strony i czy przy tej sposobności nie naruszył przepisów prawa. Przy tego rodzaju skargach konieczna była analiza okoliczności, czy zakres przedmiotowy postępowania przed organem określa żądanie skierowane uprzednio do administratora, a nie sama skarga do organu. Skarga powinna być bowiem kierowana do organu dopiero w przypadku niezrealizowania przez administratora skierowanego do niego żądania. Tym samym modyfikowanie żądania udostępnienia danych (zakresu lub celu) na etapie wniesienia skargi do organu lub w trakcie prowadzonego postepowania nie może wywołać pożądanych skutków.

[82] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2018 r. poz. 1025) – dalej: Kodeks cywilny.

[83] Decyzja Prezesa UODO z 29.11.2018 r., sygn. ZSPR.440.67.2018., decyzja Prezesa UODO z 27.11.2018 r. sygn. ZSPR.440.1208.2018., decyzja GIODO z 24.04. 2018 r. sygn. DOLiS-440-1970/16.

Oznacza to również, że wyjawienie dopiero w toku postępowania administracyjnego faktycznego celu pozyskania danych przez wnioskującego, który w swojej istocie należałoby uznać za cel uzasadniony nie może skutkować decyzją nakazującą administratorowi udostępnienie żądanych danych. Jednocześnie do wniosku skarżącego organ przychylał się wtedy, gdy przedstawiany przez wnioskującego cel pozyskania danych był rzeczywisty, a nie był jedynie pretekstem do pozyskania danych celem wykorzystania ich w innym, niż wskazywany w żądaniu celu.

Zatem dla organu ochrony danych osobowych nie była wystarczająca sama chęć wytoczenia powództwa do sądu powszechnego przeciwko osobie, której dane dotyczą[84], ponieważ na zasadność udostępnienia danych muszą wskazywać okoliczności faktyczne w sprawie. Ponadto sam cel pozyskania powinien być określony w sposób precyzyjny, natomiast okoliczności powoływane przez wnioskodawcę powinny jednocześnie uzasadniać udostępnienie danych skarżącemu w koniecznym do tego celu zakresie.

Z drugiej jednak strony organ ochrony danych osobowych oceniał także takie sytuacje gdy administratorzy, w obawie przed nieuprawnionym udostępnieniem danych osobowych osób nie udostępniali ich na żądanie skarżących, pomimo spełnienia przesłanek uprawniających skarżących do żądania tych danych. Administratorzy wykazują się zwykle daleko idącą ostrożnością w tym względzie, pozostawiając ocenę zasadności udostępnienia danych osobowych rozstrzygnięciu organu ochrony danych osobowych.

Zgodnie z obowiązującymi przepisami, przy udostępnianiu informacji o osobach korzystających z forów internetowych należy mieć także na uwadze ochronę innych praw i wolności jak np. wolność wypowiedzi. Ochrona wolności wypowiedzi nie ma jednak charakteru bezwzględnego. Warunkami odstąpienia od ochrony danych osobowych w tym zakresie może być np. proporcjonalność środków i celów oraz równowaga pomiędzy ochroną wolności wypowiedzi, ochrona czci i godności. Ocena taka wiąże się również z kwestią uprawdopodobnienia roszczenia oraz skierowania go na drogę sądową[85]. Odmowa udostępnienia danych osobowych może nastąpić dopiero po dokonaniu oceny zasadności żądania[86].

Tajemnica telekomunikacyjna

Co do zasady, w przypadku gdy podmiot, który wniósł o udostępnienie mu danych osobowych, legitymuje się przesłanką uprawniającą go do ich pozyskania, administrator danych jest zobowiązany udostępnić żądane dane osobowe. Jednakże ustawodawca przewidział sytuacje, w których administrator jest uprawniony do ich udostępnienia jedynie w przypadkach przewidzianych przepisami ustawy szczególnej.

Przykładem takiego uregulowania są przepisy dotyczące tajemnicy telekomunikacyjnej oraz dostępu do niej. Zgodnie z przepisami Prawa telekomunikacyjnego zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

W ocenie organu nadzorczego ustawodawca w ten sposób określił zamknięty krąg podmiotów, na rzecz których możliwe jest udostępnienie danych osobowych objętych tajemnicą telekomunikacyjną. W przypadku gdy podmiot zwraca się do organu o nakazanie przedsiębiorcy telekomunikacyjnemu udostępnienia danych osobowych objętych tajemnicą telekomunikacyjną, Prezes UODO odmawia uwzględnienia takiego wniosku[87].

---

[84] por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 14 kwietnia 2014 r., sygn. akt II SA/Wa 2093/13

[85] por. wyrok Naczelnego Sądu Administracyjnego z dnia 22 marca 2018 r., sygn. akt I OSK 454/16

[86] por. wyrok Naczelnego Sądu Administracyjnego z dnia 11 grudnia 2018 r., sygn. akt I OSK 398/17

[87] Decyzja Prezesa UODO z 31.10.2018 r., sygn. ZSPR.440.67.2018.

Prawo telekomunikacyjne[88] **a kserokopia dowodów osobistych**

Prezes UODO w wydawanych rozstrzygnięciach nie zgadzał się ze stanowiskiem operatora telekomunikacyjnego, że art. 161 ust. 2 pkt 7 czy też art. 57 ust. 2 Prawa telekomunikacyjnego uprawniają dostawcę publicznie dostępnych usług telekomunikacyjnych do przetwarzania danych dotyczących użytkownika będącego osobą fizyczną zawartych w dokumencie tożsamości, a wykraczających poza zakres określony w art. 161 ust. 2 Prawa telekomunikacyjnego. W swoich rozstrzygnięciach organ nadzorczy uznaje, że takie stanowisko przedsiębiorców telekomunikacyjnych jest poglądem błędnym.

Przepisy uprawniają dostawcę publicznie dostępnych usług telekomunikacyjnych do przetwarzania danych dotyczących użytkownika będącego osobą fizyczną zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych. Jednak dokumenty tożsamości, jak i dokumenty potwierdzające tożsamość, nie są dokumentami, które potwierdzałyby zdolność do wykonania zobowiązania pieniężnego. Legitymacja ZUS nie stanowi dowodu tożsamości, lecz jest dokumentem, który poświadcza uprawnienia wynikające z ustawy o systemie ubezpieczeń społecznych. Legitymacja imienna emeryta lub rencisty wystawiana jest osobom uprawnionym do emerytur i rent z ubezpieczeń społecznych oraz potwierdza status emeryta lub rencisty.

Zatem dane takie można przetwarzać zgodnie z przepisami Prawa telekomunikacyjnego wyznaczającymi zakres i cel przetwarzania danych osobowych albo za zgodą klienta, a nie przez dokonanie kopii dokumentów zawierających takie dane. Dokonanie kopii powoduje bowiem objęcie przetwarzaniem nieadekwatnego zakresu danych osobowych. Spółka nie może ograniczać prawa klienta do dowolnego sposobu zawarcia umowy, a jakiekolwiek działania wykraczające poza zakres art. 161 ust. 2 Prawa telekomunikacyjnego są niedopuszczalne.

Przedsiębiorca telekomunikacyjny może bez zgody klienta przetwarzać jedynie takie dane osobowe, które zostały wskazane w katalogu określonym w art. 161 ust. 2 Prawa telekomunikacyjnego. W przepisie tym nie zawarto zezwolenia na przetwarzanie takich danych osobowych, jak: wizerunek twarzy, płeć, dane dotyczące dowodu osobistego, w tym datę wydania, datę ważności, oznaczenie organu wydającego dowód osobisty (ewentualnie podpis, rysopis, w przypadku starszych dokumentów tożsamości).

Tajemnica bankowa

GIODO, a później Prezes UODO, prowadził sprawy związane z kwestionowaniem przez skarżących przetwarzania ich danych osobowych przez banki w zbiorach danych podmiotów, o których mowa w art. 105 ust. 4 Prawa bankowego. Są to jedne z najczęściej i najliczniej wnoszonych skarg w odniesieniu do sektora bankowego[89]. Skargi te dotyczą w głównej mierze przetwarzania danych osobowych dłużników w zbiorach danych dłużników, którzy nie wywiązali się ze zobowiązań wobec banku.

Jednakże, żeby było możliwe przetwarzanie danych osobowych osoby fizycznej na podstawie przepisu Prawa bankowego, konieczne jest zwrócenie się przez bank do dłużnika z informacją o zamiarze przetwarzania jego danych osobowych bez jego zgody, gdy nie wykonał on zobowiązania lub dopuścił się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem, a po zaistnieniu tych okoliczności powinno upłynąć co najmniej 30 dni od poinformowania tej osoby przez bank, o zamiarze przetwarzania dotyczących jej informacji, bez jej zgody. Z drugiej

[88] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954) – dalej: Prawo telekomunikacyjne.

[89] Decyzja Prezesa UODO z 7.12.2018 r. sygn. ZSPR.440.1552.2018.; Decyzja GIODO z 23.02.2018 r. sygn. DOLiS-440-1884/17, Decyzja GIODO z 15.03. 2018 r. sygn. DOLiS-440-1720/14.

strony skarżący najczęściej wskazują, że bank nie poinformował ich o okolicznościach wskazanych powyżej.

Banki zazwyczaj nie dysponują dowodem doręczenia skarżącemu wskazywanej informacji, przedkładając w postępowaniu przed organem wydruki z wewnętrznych systemów mających wskazywać na okoliczność skierowania do skarżącego ww. informacji, które to dowody nie są uznawane za wystarczające z uwagi na gwarancyjny charakter przepisów prawa bankowego. Stanowisko GIODO dotyczące konieczności możliwego do udowodnienia powiadomienia skarżących o zamiarze przetwarzania ich danych osobowych w rozmaitych bazach dłużników, najlepiej przy użyciu listu poleconego ze zwrotnym poświadczeniem odbioru, zostało potwierdzone w wyrokach sądów administracyjnych[90].

Konieczna jest zatem zmiana podejścia podmiotów sektora bankowego do informowania osób fizycznych o okolicznościach z art. 105a ust. 3 Prawa bankowego w taki sposób, aby następowało rzeczywiste poinformowanie osób o zamiarze przetwarzania przez bank danych osobowych oraz dysponowały one dowodami potwierdzającymi tę okoliczność. O ile bowiem ustawodawca nie ograniczył sposobów i form zawiadomienia osoby fizycznej na podstawie art. 105a ust. 3 Prawa bankowego, o tyle w każdym wypadku sposób taki powinien umożliwić zweryfikowanie faktu poinformowania klienta banku o zamierzonym przetwarzaniu jego danych osobowych lub też przynajmniej potwierdzenie, że klientowi umożliwiono zapoznanie się z taką informacją[91].

Marketing

W dalszym ciągu do UODO wpływają skargi dotyczące przetwarzania danych osobowych w celach marketingowych bez zgody osoby, której dane dotyczą. Zauważyć jednocześnie należy, że niektórzy z administratorów błędnie podchodzą do kwestii wyrażonych sprzeciwów dotyczących marketingu własnych produktów i usług, uznając, że ich klienci godzą się w sposób dorozumiany na przetwarzanie danych osobowych w celach marketingowych. Tytułem przykładu, administrator przy zawieraniu umowy o świadczenie usług telekomunikacyjnych, wprowadził do wzorca umowy rubrykę dotyczącą wyrażenia zgody na przetwarzanie danych osobowych w celu marketingu produktów i usług. Ustalono, że skarżący już przy zawieraniu umowy zaznaczył rubrykę „NIE", a tym samym, w sposób jednoznaczny wyraził swoją wolę, co do nieprzetwarzania jego danych osobowych w celu marketingu własnych produktów i usług.

Wskazać jednocześnie należy, że niektórzy z administratorów w dalszym ciągu nie kwalifikują informacji o możliwości uaktywnienia usługi polegającej na otrzymywaniu informacji o bieżących promocjach, jako marketingu własnych produktów i usług. W ocenie Prezesa UODO, w przypadku, gdy dane osobowe są przetwarzane w celu kierowania informacji mającej nakłonić klienta lub potencjalnego klienta do skorzystania z oferowanych usług, to tego rodzaju przetwarzanie stanowi cel marketingowy. W przypadku zatem wyrażenia sprzeciwu przez osobę, której dane dotyczą, administrator jest zobowiązany do zaprzestania kierowania do tej osoby marketingu produktów własnych i usług, niezależnie od tego, jaka usługa jest przedmiotem marketingu[92].

---

[90] W wyroku z 25 lipca 2017 r. sygn. akt I OSK 2859/16 NSA, oraz w wyroku II SA/Wa 1957/17 Sąd wskazał, cyt. „Przede wszystkim zwrócić uwagę należało na materialny (ochronny), a nie formalny charakter tego przepisu. Wymaga on w sposób kategoryczny poinformowania, a nie wysłania zawiadomienia, jak zdaje się twierdzić bank w swoim stanowisku procesowym".

[91] por. wyrok Naczelnego Sądu Administracyjnego z dnia 7 sierpnia 2018 r., sygn. akt I OSK 2051/16

[92] Por. Decyzja Prezesa UODO z 7.09.2018 r., sygn. ZSPR.440.394.2018., Decyzja Prezesa UODO z 21.12.2018 r. sygn. ZSPR.440.854.2018., decyzja Prezesa UODO z 20.12.2018. ZSPR.440.370.2018., decyzja Prezesa UODO z 12.12.2018 r., sygn. ZSPR.195.2018., decyzja Prezesa UODO z 1.12.2018 r. sygn. ZSPR.440.779.2018., decyzja Prezesa UODO z 10.10.2018 r. sygn. ZSPR.440.1170.2018., decyzja Prezesa UODO z 14.12.2018 r. sygn. ZSPR.440.815.2018.

Innym charakterystycznym przykładem była sytuacja, w której skarżący postanowił zrezygnować z otrzymywania jakiejkolwiek informacji marketingowej od banku, którego był klientem. W rezultacie ustalono, że złożenie przez zainteresowanego sprzeciwu oznacza, że nie powinien on na swoim koncie internetowym, do którego się loguje, otrzymywać jakichkolwiek informacji o marketingu. W przeciwnym wypadku można bowiem uznać, że bank przetwarza dane osobowe skarżącego w celach marketingowych. Bank w sposób jednoznaczny nawoływał do podjęcia aktywności przez klienta, gdyż wyświetlanie w odpowiedniej zakładce informacje o całkiem nowych produktach własnych, stanowi nakłanianie klienta do zawarcia umowy z bankiem[93].

Tym samym należy uznać, że banki nie powinny nakłaniać swoich klientów, o ile ci nie wyrazili zgody na przetwarzanie danych osobowych w celach marketingowych, do korzystania z dodatkowych usług za pomocą prezentowanych w Internecie treści marketingowych oraz reklamowych.

Ubezpieczenia

Pośród tematów, którymi UODO zajmował się podczas postępowań prowadzonych na podstawie skarg wobec towarzystw ubezpieczeniowych, należy wymienić:

- pozyskiwanie zbyt dużego zakresu danych osobowych, nieadekwatnego do potrzeb, a często na zapas, w tym danych dotyczących zdrowia;
- niewystarczający poziom spełniania obowiązków informacyjnych – informacje w opinii skarżących są niejasne i zbyt ogólne;
- przekazywanie lub powierzanie danych osobowych do podmiotów trzecich w celach windykacyjnych;
- niedostateczne informowanie klientów o podstawach prawnych przetwarzania danych po ustaniu umowy ubezpieczenia, towarzystwa ubezpieczeń na życie, dotyczących ich zdrowia, przekazywania lub powierzania ich podmiotom trzecim;
- wysyłanie informacji handlowej i marketingowej bez wymaganych zgód oraz wbrew wyrażonym sprzeciwom;
- sposób konstruowania wniosków o ubezpieczenie;
- wdrożenia nieodpowiednich procedur przez towarzystwa ubezpieczeniowe;
- wymuszanie udzielania zgód, jako warunku zawarcia ubezpieczenia, w sytuacji ich pełnej dobrowolności;
- przetwarzanie danych osobowych przez agentów ubezpieczeniowych, którzy nieprawidłowo identyfikują osoby wnioskujące o zawarcie ubezpieczenia, czy wykorzystują posiadane dane osobowe klientów towarzystw ubezpieczeniowych w celu zawierania fikcyjnych umów, ujawnianie danych osobowych ubezpieczonych osób fizycznych podmiotom i osobom trzecim z zakwestionowaną przez skarżących podstawą prawną (np. dla celu publikacji, likwidacji szkody);
- przetwarzanie danych osobowych w celu wystawiania polis ubezpieczeniowych OC komunikacyjnej, jako kontynuacji: po wygaśnięciu polisy i braku jej wypowiedzenia, oraz po przejściu własności pojazdu.

Nie można określić, które z powyższych zagadnień dominują wśród rozpatrywanych spraw, gdyż są to na ogół pojedyncze i nieliczne przypadki. Można się spodziewać, że rosnąca świadomość obywateli prowadzić będzie do coraz częstszego kwestionowania konieczności pozyskiwania szerokiego zakresu danych osobowych, bez wyraźnego uzasadnienia, w szczególności danych dotyczących zdrowia i życia.

Towarzystwa będą zmuszone do zmodyfikowania swojej polityki informacyjnej, gdyż ich klienci z jednej strony nie znają i kontestują przepisy prawa, które nakładają nakładające na towarzystwa ubezpieczeniowe obowiązki związane z przetwarzaniem danych, ale też stanowiące podstawy prawne

[93] por. wyrok Naczelnego Sądu Administracyjnego z 5 grudnia 2018 r., sygn. akt I OSK 53/17 w odniesieniu do decyzji GIODO z dnia 16.12.2015 r. sygn. DOLiS-440-285/15 (DOLIS/DEC-440-960/15).

do ich pozyskiwania i przetwarzania. Szczególnie istotne jest informowanie o podstawach prawnych i celach przetwarzania danych po upływie okresu ubezpieczenia.

Operatorzy pocztowi oraz firmy kurierskie

Do UODO wpływają skargi dotyczące szeroko pojętych usług kurierskich i pocztowych. Obejmują one w przeważającym zakresie problematykę ujawnienia danych osobowych zawartych na przesyłkach poprzez doręczenie osobom nieuprawnionym (w tym pozostawienie na portierni lub u ochrony osiedla, nie wrzucenie korespondencji do skrzynki). Takie działania powodują ryzyko ujawnienia osobom nieuprawnionym danych osobowych zawartych w przesyłkach w przypadku ich niedoręczenia i zagubienia przez podmioty realizujące usługę.

Przedmiotem analizy w postępowaniach jest kwestia legalności przetwarzania danych osobowych znajdujących się na przesyłkach oraz szeroko ujmowany aspekt ich zabezpieczenia (zarówno danych przesyłanych na, jak i w przesyłce). Dodatkową kwestią jest specyfika usług świadczonych przez podmioty, tj. przesyłki zwykłe (nierejestrowane), rejestrowane oraz przesyłki kurierskie (w większości zawierające dane osobowe, np. na fakturach), która powoduje, że nie wszystkie przesyłki są monitorowane poprzez usługę „śledzenie przesyłek", i wątpliwym jest ustalenie, czy przesyłkę zagubiono lub doręczono ją do innego adresata, np. zwykłym listem.

Co do legalności przetwarzania danych zawartych na przesyłce nie budzi ona wątpliwości – przetwarzanie tych danych jest niezbędne do realizacji umowy przewozu.

Inną kwestią jest ochrona danych osobowych znajdujących się w przesyłce. Należy zauważyć, że podmiot realizujący usługę, w przeważającej liczbie przypadków nie ma wiedzy, jakie informacje, w tym dane osobowe, są nimi objęte, jakie dane osobowe, zawiera list lub paczka (szczególnie dotyczy to małych podmiotów lub klientów indywidulnych).

W związku z powyższym najwięcej wątpliwości występuje w tym zakresie co do określenia:

- czy i w odniesieniu do jakich danych osobowych operatorowi usług pocztowych przysługuje status administratora w rozumieniu art. 4 pkt 7 rozporządzenia 2016/679,
- jaki podmiot ponosi odpowiedzialność za naruszenie rozporządzenia 2016/679 w przypadku ujawnienia danych zawartych w niedoręczonych – zagubionych przesyłkach (o których to danych często podmiot doręczający nie wie).

Samorządy zawodowe

Do UODO wpływają także skargi dotyczące przetwarzania danych dotyczących osób fizycznych w związku z wykonywaniem przez komorników, adwokatów zadań z zakresu prowadzonej przez nich działalności. Uprzednio podstawy prawne do przetwarzania danych przez te podmioty także były przedmiotem analizy Generalnego Inspektora Ochrony Danych Osobowych[94].

Adwokat, który przetwarza dane osobowe osób trzecich, pozyskane od swoich klientów, nie musi powiadamiać tych osób o zbieraniu i przetwarzaniu ich danych, gdyby naruszało to tajemnicę zawodową. Taka osoba trzecia nie może złożyć sprzeciwu wobec przetwarzania jego danych przez adwokata, jeśli dane osobowe pozyskane zostały przez adwokata w związku z udzielaniem pomocy prawnej.

W przypadku danych osobowych przetwarzanych przez organy adwokatury oraz organy izb adwokackich w zakresie niezbędnym do prawidłowej realizacji zadań publicznych określonych w ustawach oraz danych osobowych przetwarzanych w ramach nadzoru nad tym samorządem zawodowym istnieją podstawy prawne do przetwarzania danych w oparciu o przepisy Prawa

[94] Decyzja GIODO z 27.02.2018 r. sygn. DOLiS-440-46/15

o adwokaturze, czy też przepisy nakładające na te podmioty określone obowiązki, choćby wynikające z Ordynacji podatkowej[95], czy też przepisów ustawy o rachunkowości[96].

Kolejną kategorią skarg wpływających do UODO są te, które dotyczą **przetwarzania danych przez komorników sądowych**. Komornik sądowy, prowadząc postępowania egzekucyjne gromadzi, przetwarza, ustala cele i sposoby przetwarzania danych osobowych osób fizycznych. Jest administratorem danych osobowych, a tym samym ma obowiązek stosowania przepisów ogólnego rozporządzenia oraz przepisów krajowych dotyczących ochrony danych osobowych. Komornik sądowy przetwarza dane osobowe stron i uczestników postępowania na podstawie przepisów prawa.

Zgodnie z motywem 68 rozporządzenia prawa do przenoszenia nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Kodeks postępowania cywilnego[97], jak i ustawa o komornikach sądowych[98] w sposób konkretny, wyraźny i prawnie uzasadniony nakładają na komornika sądowego obowiązek gromadzenia danych osobowych dłużników, uczestników postępowania egzekucyjnego, a w niektórych przypadkach dają możliwość ich gromadzenia, wypełniając przesłankę przetwarzania danych osobowych wyrażoną w art. 6 ust. 1 lit. c rozporządzenia 2016/679.

Przetwarzanie przez komorników sądowych pozyskanych danych osobowych dokonywane jest w celu i zakresie niezbędnym do wykonywania zadań nałożonych na nich przepisami prawa oraz w celu prawidłowego funkcjonowania kancelarii. Dane przetwarzane są do czasu prawomocnego zakończenia postępowania egzekucyjnego, zabezpieczającego lub postępowania innego rodzaju, a po jego zakończeniu na podstawie art. 164 o komornikach sądowych w zw. z § 7 rozporządzenia Ministra Sprawiedliwości z dnia 14 grudnia 2018 r. w sprawie przechowywania i niszczenia akt spraw komorniczych oraz zamkniętych urządzeń ewidencyjnych[99] przez okres wskazany w ww. paragrafie.

Zgodnie z § 12 ww. rozporządzenia akta spraw prawomocnie zakończonych przed dniem wejścia w życie ww. rozporządzenia kwalifikuje się na podstawie przepisów dotychczasowych. Czas przechowywania wiadomości e-mail i dokumentacji elektronicznej jest dostosowany do okresu przechowywania dokumentacji papierowej. Zatem regulacje wynikające z innych ustaw nakazują przechowywanie dokumentów przez określony czas, niezależnie od wytycznych rozporządzenia 2016/679[100].

Brokerzy danych

Kolejną kategorią podmiotów, które pozostają w zainteresowaniu organu nadzorczego, są **brokerzy danych**. Za brokera danych uważany jest podmiot zajmujący się masowym zbieraniem danych osobowych oraz ich udostępnianiem (za odpłatą) podmiotom trzecim.

Brokerów możemy podzielić na brokerów danych osób prowadzących działalność gospodarczą oraz brokerów danych osobowych, osób fizycznych których dane nie zostały pozyskane w związku z prowadzaną przez nich działalnością.

---

[95] Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2019 r. poz. 900) – dalej: Ordynacja podatkowa.

[96] Art. 10 ust. 1 pkt 4 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2019 r. poz. 351) – dalej: ustawa o rachunkowości; nakładający wymóg wywiązania się z prawnego obowiązku związanego z prowadzeniem rachunkowości dotyczącego rozliczenia podatku i przechowywania danych księgowych.

[97] Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2018 r. poz. 1360 z późn. zm) – dalej: k.p.c.

[98] Ustawa z dnia 22 marca 2018 r. o komornikach sądowych (Dz. U. z 2018 r. poz. 771) – dalej: ustawa o komornikach sądowych.

[99] Rozporządzenie Ministra Sprawiedliwości z dnia 14 grudnia 2018 r. w sprawie przechowywania i niszczenia akt spraw komorniczych oraz zamkniętych urządzeń ewidencyjnych (Dz. U. z 2018 r. poz. 2408).

[100] Decyzja GIODO z dnia 27.02.2018 r. sygn. DOLiS-440-46/15.

Do pierwszej grupy podmiotów można zaliczyć spółki, które pozyskują dane osobowe z rejestrów jawnych (np. Centralnej Ewidencji i Informacja o Działalności Gospodarczej – CEIDG).

Do drugiej grupy podmiotów z tej kategorii można zaliczyć spółki, które zajmują się pozyskiwaniem danych osobowych osób fizycznych poprzez prowadzenie ankiet, konkursów, quizów, sondaży itp. Dane osobowe respondentów (imię, nazwisko, adres, telefon, e-mail, data urodzenia) pozyskiwane są w wyniku udzielenia odpowiedzi na kilka pytań. Na podstawie zebranych danych spółka profiluje osoby (adres, wiek, płeć), których dane posiada i czasowo je udostępnia podmiotowi trzeciemu, który złożył stosowne zamówienie.

W trakcie prowadzonych postępowań UODO badał legalność przetwarzania danych osobowych przez brokerów danych. Postępowania wyjaśniające ujawniły naruszenia przepisów w zakresie pozyskiwania zgód osób, których dane dotyczą, oraz spełnienia obowiązków informacyjnych[101].

Prowadzenia ukrytych rekrutacji

Prowadzenie procesów rekrutacyjnych, w których pracodawca wykorzystując portale internetowe, pośredniczące w rekrutacji, zastrzega sobie anonimowość, jest niezgodne z przepisami o ochronie danych osobowych. Prezes UODO wielokrotnie podkreślał, że powyższe ma szczególne znaczenie w związku z sytuacjami, w których ogłoszenia o pracę mogą być sposobem na wyłudzanie danych osobowych przez nieuczciwe podmioty do własnych celów niezwiązanych z zatrudnianiem pracowników.

W związku z prowadzeniem tzw. „ukrytych rekrutacji" kandydaci do pracy nie posiadają wiedzy, jaki podmiot zbiera ich dane osobowe i wobec jakiego podmiotu mogą realizować swoje prawa. O prawidłowym wykonaniu obowiązku informacyjnego, nie możemy mówić również w sytuacji, gdy klauzula informacyjna zostanie wysłana przez potencjalnego pracodawcę w odpowiedzi na otrzymaną aplikację, ponieważ obowiązek poinformowania m.in. o tożsamości pracodawcy powinien być realizowany przez niego na etapie zbierania danych osobowych, a nie na etapie ich utrwalania. Osoba przekazująca dane osobowe powinna posiadać wiedzę odnośnie do tego, komu je udostępnia[102].

Wykorzystywanie przez pracowników danych osobowych, do których mają dostęp w ramach wykonywania obowiązków służbowych, dla innych celów

Podobnie jak w latach ubiegłych, także w 2018 r. do organu ochrony danych osobowych zgłaszano skargi dotyczące wykorzystania danych osobowych przez zatrudnionego u danego administratora pracownika w celu innym niż ten, dla którego dane osobowe zostały przez administratora pozyskane. Skargi powyższe dotyczą najczęściej sytuacji, gdy pracownik bez wiedzy pracodawcy pozyskuje dane, mając do nich dostęp w związku z wykonywaniem obowiązków służbowych.

Organ wielokrotnie podkreślał, że pracodawca jako administrator danych osobowych ponosi odpowiedzialność za przetwarzanie danych osobowych, w tym za ich należyte zabezpieczenie oraz za prawidłowe wykorzystywanie ich przez zatrudnionych przez siebie pracowników. Wskazać należy, że w świetle przepisów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, tj. na podstawie art. 36 ust. 1, administrator był obowiązany stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

[101] Prezes UODO w dniu 27.11.2018 r. wydał decyzję nakazującą (sygn. ZSPR.K.421.10.2018/21833/MN) usunięcie uchybień spółce w wyniku przeprowadzonej kontroli (DIS-K-421/193/17).

[102] ZSZZS.440.72.2018

Zgodnie zaś z art. 38 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych administrator był obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu były przekazywane. W konsekwencji, pozyskanie danych osobowych przez pracownika administratora w związku z wykonywaniem obowiązków służbowych, a następnie wykorzystanie tych danych w celu innym, niż cel, dla którego zostały one zebrane stanowi naruszenie przepisów ustawy o ochronie danych osobowych, nawet w przypadku, gdy wykorzystanie to nastąpiło bez wiedzy administratora. Takie wykorzystanie świadczy o niesprawowaniu przez administratora należytej kontroli nad przetwarzaniem danych osobowych[103] (podobnie Naczelny Sąd Administracyjny w wyroku z 4 kwietnia 2003 r.[104]).

Udostępnienie danych osobowych pracowników osobom nieupoważnionym

Do organu wpływają m.in. skargi dotyczące istotnej dla ochrony danych osobowych pracowników kwestii wręczania im dokumentów dotyczących rozwiązania stosunku pracy w obecności innych osób. Przepisy Kodeksu pracy określają sposób postępowania pracodawców przy udzielaniu kar porządkowych i wypowiadaniu umowy o pracę. Nie przewidują one jednak uprawnienia pracodawcy do dokonywania powyższych czynności w obecności innych pracowników. Podkreślenia wymaga także, że jednym z podstawowych obowiązków pracodawcy zaliczanych do zasad prawa pracy jest poszanowanie godności oraz prywatności pracownika jako jego dóbr osobistych. Informacje dotyczące pracowników, w tym dotyczące określonych zdarzeń takich, jak wypowiedzenie umowy o pracę lub udzielenie kary porządkowej, mogą być dostępne jedynie dla ograniczonego kręgu osób upoważnionych u danego pracodawcy.

Realizacja przez pracowników prawa dostępu do swoich danych

Również w 2018 r. do organu ochrony danych osobowych były kierowane skargi dotyczące realizacji przez pracodawców żądań pracowników dotyczących dostępu do swoich danych zarówno zgodnie z art. 32 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, jak i z art. 15 ust. 1 RODO. Niemniej żeby organ mógł nakazać pracodawcy udostępnienie pracownikowi informacji o jego danych, konieczne jest uprzednie zwrócenie się przez niego z takim żądaniem do pracodawcy. Brak takiego działania lub zbyt szeroki zakres żądania skutkuje tym, że nie jest możliwe wydanie przez organ nakazu w tym zakresie[105]. Podkreślenia wymaga, że organ ochrony danych osobowych nie może wydawać rozstrzygnięć w zakresie do dokumentów, a rozstrzygnięcia te mogą dotyczyć wyłącznie danych osobowych w tych dokumentach zawartych.

Kontrola wykorzystywania zwolnień lekarskich

Należy także odnotować skargi dotyczące kontroli wykorzystania zwolnień lekarskich. Pracownicy skarżyli się na to, że kontroli dokonywali pracownicy podmiotów zewnętrznych, nie zaś pracodawcy. Jednakże należy stwierdzić, że obowiązujące przepisy prawne nie ograniczają możliwości powierzenia przez pracodawcę przeprowadzenia kontroli wykorzystania zwolnienia lekarskiego niezgodnie z jego celem podmiotowi zewnętrznemu. Warto również wskazać, że takie podmioty zewnętrzne, uprawnione są do przetwarzania danych osobowych osób kontrolowanych, o ile pracodawca zawrze z nimi umowę powierzenia przetwarzania danych osobowych. Kontrola powinna zostać przeprowadzona przez osoby posiadające do tego imienne upoważnienia, które są zgodne ze wzorem upoważnienia określonego w rozporządzeniu Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu kontroli prawidłowości

[103] ZSZZS.440.93.2018

[104] Wyrok NSA z 4 kwietnia 2003 r., sygn. akt II SA 2935/02

[105] DOLiS-440-130/16/II

wykorzystania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich[106]. Ponadto pracodawca może przekazać osobom kontrolującym dane osobowe pracownika w zakresie wynikającym z umowy powierzenia przetwarzania danych osobowych i niezbędnym do przeprowadzenia kontroli wykorzystania zwolnienia lekarskiego[107].

Udostępnienie danych osobowych pacjentów osobom nieupoważnionym

Należy odnotować skargi związane z przesyłaniem przez podmioty lecznicze do rodziców małoletnich dzieci wezwań do zgłoszenia się w celu szczepień, przy czym wezwania te wysyłane były bez kopert, w związku z czym osoby postronne mogły zapoznać się z ich treścią, a tym samym z danymi osobowymi zarówno rodziców, do których adresowano wezwanie, jak i ich dzieci. W powyższych skargach wskazywano, że zawarte w wezwaniach do szczepień dane osobowe małoletnich dotyczyły m.in. ich imienia, nazwiska, roku urodzenia oraz informacji jakie szczepienia nie zostały dotychczas wykonane. W ocenie organu ochrony danych osobowych administrator odpowiedzialny jest za zabezpieczenie danych osobowych oraz przetwarzanie ich zgodnie z przepisami o ochronie danych osobowych, w tym również za działania pracowników w powyższym zakresie. W rozstrzygnięciu wydanym w takiej sprawie organ ochrony danych osobowych zakwestionował powyższą praktykę i wskazał, że przesyłając wezwanie do szczepień za pośrednictwem poczty tradycyjnej bez koperty, administrator nie zabezpieczył w sposób właściwy danych osobowych matki i jej małoletnich dzieci, a co za tym idzie umożliwił do nich dostęp osobom nieuprawnionym i naruszył tym samym art. 36 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych[108].

W skargach kierowanych do organu ochrony danych osobowych pacjenci kwestionują także przetwarzanie ich danych osobowych zawartych w dokumentacji medycznej przez personel niemedyczny[109]. Jednakże wskazać należy, że zgodnie z art. 24 ust. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[110] do przetwarzania danych zawartych w dokumentacji medycznej, o której mowa w art. 25 ust. 1 tej ustawy, w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, poza osobami wykonującymi zawód medyczny są uprawnione także inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora. Wobec powyższego należy podkreślić, że wspomniane powyżej osoby mogą przetwarzać dane zawarte w dokumentacji medycznej, o ile następuje to w określonych we wskazanym powyżej przepisie celach, pod warunkiem udzielenia im przez administratora stosownego upoważnienia, które w sposób jednoznaczny określać powinno dozwolony zakres przetwarzania danych.

Przetwarzanie danych osobowych dzieci i rodziców w związku z obowiązkowymi szczepieniami ochronnymi

---

[106] Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich (Dz.U. z 1999 r. Nr 657, poz. 43).

[107] ZSZZS.440.526.2018

[108] ZSZZS.440.124.2018

[109] ZSZZS.440.196.2018

[110] Ustawa z dnia 16 listopada 2006 r. o prawach pacjenta i Rzeczniku Praw Pacjenta(t.j. Dz. U. z 2017 r. poz. 1318 z późn. zm.).

Należy wskazać, że w roku 2018 utrzymał się trend składania skarg na przetwarzanie danych osobowych rodziców oraz ich małoletnich dzieci przez podmioty wykonujące działalność leczniczą i Państwową Inspekcję Sanitarną. Przede wszystkim w tego rodzaju sprawach skarżący kwestionują udostępnienie ich danych osobowych (w tym danych o niezaszczepieniu dziecka, tj. danych o stanie zdrowia) właściwemu miejscowo państwowemu powiatowemu inspektorowi sanitarnemu.

W tego rodzaju sprawach opiekunowie prawni małoletnich dzieci wskazują na brak podstaw prawnych do przetwarzania danych osobowych ich dzieci w celu wykonania obowiązku szczepień[111]. Podobnie jak robił to wcześniej GIODO, Prezes UODO podkreśla jednak w wydawanych decyzjach, że przetwarzanie danych osobowych w celu egzekwowania wykonania obowiązku szczepień znajduje oparcie w powszechnie obowiązujących przepisach prawa. Przepisy ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi nakładają na osoby przeprowadzające szczepienia ochronne szereg związanych z tą okolicznością obowiązków (art. 17 ust. 8 ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi[112], m.in. dokonywania wpisów potwierdzających wykonanie szczepienia, sporządzania sprawozdania z przeprowadzonych szczepień ochronnych oraz sporządzania sprawozdania ze stanu zaszczepienia osób objętych profilaktyczną opieka zdrowotną, które następnie osoby prowadzące szczepienia ochronne zobowiązane są przekazać państwowemu powiatowemu inspektorowi sanitarnemu[113].

Istotne jest jednak rozgraniczenie zakresu danych osobowych przekazywanych przez osoby prowadzące szczepienia ochronne na rzecz państwowego powiatowego inspektora sanitarnego. Wspomniane wyżej sprawozdanie, sporządzane na podstawie art. 17 ust. 8 pkt 2 u.z.z. powinno zawierać dane niezbędne do wysłania przez odpowiedni oddział Państwowej Inspekcji Sanitarnej upomnienia wzywającego do wykonania obowiązku szczepiennego oraz podejmowania dalszych czynności egzekucyjnych w przypadku niewykonania obowiązku. Podkreślić bowiem należy, że dane zarówno pozyskiwane przez państwowego powiatowego inspektora sanitarnego, jak i mu udostępniane muszą być również wystarczające do prowadzenia przez niego skutecznej egzekucji obowiązku szczepień, w ramach której jako wierzyciel sporządza on tytuł wykonawczy. Zakres tych danych regulowany jest przez art. 27 ustawy o postępowaniu egzekucyjnym. Zauważyć należy, że dane osobowe w postaci numeru telefonu do opiekuna prawnego małoletniego dziecka nie są niezbędne do przekazania w ww. sprawozdaniu, zgodnie z zakresem danych wymaganych do wydania skutecznego tytułu egzekucyjnego. Tym samym uznać należy, że ww. dane osobowe w zakresie numeru telefonu nie mogą być przez osoby przeprowadzające szczepienia ochronne udostępniane, a w związku z brakiem podstawy prawnej zezwalającej na udostępnienie przez ww. osoby numeru telefonu, dane osobowe w zakresie numeru telefonu nie powinny być przetwarzane także przez państwowego powiatowego inspektora sanitarnego[114].

Udostępnianie danych osobowych zawartych w opinii z przebiegu terapii psychologicznej

Organ ochrony danych osobowych wielokrotnie spotykał się ze skargami dotyczącymi udostępniania danych osobowych zawartych w dokumentacji medycznej i opiniach psychologicznych po uzyskaniu pełnoletności pacjenta jego byłym opiekunom prawnym lub osobom przez tych opiekunów upoważnionym.

Wskazać należy, że z dniem uzyskania pełnoletniości uzyskuje się pełną zdolność do czynności prawnych. W ocenie Prezesa UODO nie można uznać, aby zawarte w powyższej dokumentacji dane osobowe (w tym dane dotyczące stanu zdrowia), wydane byłemu opiekunowi prawnemu

[111] ZSZZS.440.101.2018.II

[112] Ustawa z 5 grudnia 2018 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. z 2018 r. poz. 151 z późn. zm.) – dalej jako u.z.z.

[113] ZSZZS.440.87.2018

[114] ZSZZS.440.684.2018

już po ukończeniu 18. roku życia przez osobę, której dotyczą, udostępnione zostały prawidłowo, w sposób zgodny z obowiązującymi przepisami.

Przedstawiane w tego typu skargach zarzuty dotyczące udostępnienia danych osobowych, w tym również danych dotyczących stanu zdrowia, osobom nieuprawnionym uznać należy za zasadny. Zatem administrator danych osobowych pacjentów powinien zwrócić szczególną uwagę na przestrzeganie przepisów dotyczących ochrony ich danych osobowych w powyższym zakresie[115].

„Czarne listy" pacjentów

W 2018 r. zastrzeżenia Prezesa UODO wzbudziła praktyka, polegająca na tworzeniu tzw. czarnej listy pacjentów. Prezes UODO powziął informację o stworzeniu serwisu internetowego, w którym lekarze mogli sprawdzić, czy zapisany do nich pacjent nie jest tym, który spóźnia się lub w ogóle nie przychodzi na wizyty umówione u innych lekarzy.

Pacjenci identyfikowani byli na ww. liście za pośrednictwem numerów telefonów, znajdujących się w zasobach portalu, które miały służyć do zidentyfikowania dzwoniącego jako „niesolidnego pacjenta". Wobec powstałych wątpliwości co do tego rodzaju praktyki, Prezes UODO wszczął z urzędu postępowanie mające na celu sprawdzenie, czy nie narusza ona przepisów o ochronie danych osobowych oraz podjął decyzję o przeprowadzeniu kontroli w podmiocie prowadzącym ww. serwis internetowy.

Nagrywanie wizerunku ucznia podczas zajęć lekcyjnych

W 2018 r. w wyniku wniesienia środka zaskarżenia w postaci wniosku o ponowne rozpatrzenie sprawy, Prezes UODO rozstrzygał w sprawie dotyczącej skargi rodziców na przetwarzanie danych osobowych ich małoletniego dziecka przez jedną ze szkół podstawowych. W sprawie tej wskazano, że podczas zajęć lekcyjnych wizerunek oraz zachowanie małoletniego utrwalane było przy użyciu należącej do szkoły kamery, przez nauczycielkę małoletniego.

Prezes UODO potwierdził w przedmiotowej sprawie wyrażone uprzednio stanowisko GIODO wskazujące, że nie można zakwalifikować powyższych praktyk w zakresie prowadzonego przez administratora procesu przetwarzania danych osobowych jako zgodnych z przepisami o ochronie danych osobowych, gdyż brak jest podstawy prawnej dla pozyskania ww. danych osobowych małoletniego. Artykuł 108a Prawa oświatowego[116] przewiduje możliwość stosowania monitoringu w szkołach, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia, przy czym monitoring nie może obejmować pomieszczeń, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze. Brak jest natomiast przepisów umożliwiających nagrywanie ucznia przez placówkę w trakcie zajęć w celu udokumentowania jego zachowania[117].

Policja

W omawianym okresie sprawozdawczym skargi na działania Policji dotyczyły najczęściej kwestii przetwarzania danych osobowych w bazach Krajowego Systemu Informacyjnego Policji[118] oraz w bazach Krajowego Centrum Informacji Kryminalnych[119], przy czym skarżący zarzucali Policji głównie nieudzielenie im informacji, czy ich dane osobowe są przetwarzane w KSIP lub w KCIK, a także odmowę zaprzestania przetwarzania ich danych w tych systemach.

[115] ZSZZS.440.651.2018

[116] Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2018 r. poz. 996 z późn. zm.).

[117] ZSZZS.440.208.2018.II

[118] Dalej jako: KSIP

[119] Dalej jako: KCIK

Organ ochrony danych osobowych w takich sprawach brał pod uwagę brzmienie art. 20 ustawy z dnia 6 kwietnia 1990 o Policji[120] oraz art. 2 ust. 2 ustawy z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych[121], zgodnie z którymi dane osobowe mogą być przetwarzane zarówno w KSIP, jak i w KCIK bez wiedzy i zgody osób, których te dane dotyczą. Ponadto art. 20 ustawy o Policji określa także termin przetwarzania danych oraz zasady ich usuwania z baz KSIP.

W sprawach dotyczących przetwarzania danych osobowych w KCIK uwzględniano również treść art. 14 ustawy o przetwarzaniu informacji kryminalnych, który określa dopuszczalny okres przetwarzania danych osobowych w KCIK, jak również treść art. 25 tej ustawy, który reguluje zasady usuwania danych osobowych z baz tego systemu. Istotnym jest, że wymienione wyżej przepisy obu ustaw są przepisami szczególnymi w stosunku do postanowień ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, mają zatem zastosowanie w pierwszej kolejności. Ich treść przesądza o tym, że Prezes UODO nie ma bezwzględnej, mającej zastosowanie do każdego przypadku podstawy prawnej do nakazania Komendantowi Głównemu Policji jako administratorowi systemów KSIP i KCIK udzielenia skarżącym informacji o przetwarzaniu ich danych osobowych albo ich usunięcia[122].

W świetle obowiązujących przepisów decyzje Komendanta Głównego Policji w sprawie udzielenia informacji o przetwarzaniu danych lub usunięciu danych z baz KSIP i KCIK w istocie mają charakter uznaniowy. Dotyczy to również oceny przydatności przetwarzanych danych osobowych do celów związanych z wykonywaniem zadań Policji, zgodnie z kryteriami określonymi w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 23 sierpnia 2018 r. w sprawie przetwarzania informacji przez Policję[123]. W rozdziale 5 tego aktu prawnego określono kryteria weryfikacji przechowywania w KSIP danych osobowych ze względu na ich dalszą przydatność, którymi są m.in. rodzaj i charakter popełnionego przestępstwa, rodzaj i charakter naruszonego dobra chronionego prawem, formy sprawstwa, postać zamiaru, czas, który upłynął od momentu wprowadzenia danych do zbioru, aktualność przesłanek legalności oraz niezbędności dalszego przetwarzania danych do wykonania zadań ustawowych, wystąpienie okoliczności określonych w art. 20 ust. 17b i 18 ustawy o Policji, a w przypadku danych daktyloskopijnych wystąpienie okoliczności określonych w art. 21l ust. 2 i art. 21m tej ustawy. W konsekwencji postępowania administracyjne w takich sprawach kończyły się najczęściej wydaniem decyzji nieuwzględniających żądań skarżących[124]. Należy dodać, że przedstawiane przez skarżących argumenty za zaprzestaniem przetwarzania ich danych w świetle powołanych przepisów prawa nie były zasadne. Dla przykładu skarżący powoływali się na fakt zatarcia skazania albo dobrowolnego poddania się odpowiedzialności karnej, jako przesłanki przesądzającej o ustaniu celu przetwarzania ich danych osobowych, o którym mowa w art. 25 pkt 3 ustawy o przetwarzaniu informacji kryminalnych.

Skargi kierowane do Prezesa UODO na działania Policji dotyczyły także kwestii udostępniania danych osobowych, w tym danych funkcjonariuszy, innym podmiotom, a w szczególności organom administracji publicznej lub podmiotom wykonującym zadania z zakresu administracji, jak również osobom fizycznym. Część skarg dotyczyła odmowy udostępnienia skarżącym danych osobowych funkcjonariuszy Policji w związku deklarowanym przez skarżących zamiarem wytoczenia tym funkcjonariuszom powództwa przed sądem. Takie żądania najczęściej nie były zasadne. Samo powoływanie się przez skarżących na prawnie usprawiedliwiony cel pozyskania danych osobowych funkcjonariuszy Policji nie jest bowiem wystarczającą przesłanką do wystąpienia z wnioskiem o udostępnienie przedmiotowych danych[125].

---

[120] Tj. Dz. U. z 2019 r. poz. 161 z późn. zm.

[121] Tj. Dz. U. z 2019 r. poz. 44 z późn. zm.

[122] Decyzja z 18.12.2018 r. (sygn. akt: ZSOŚS.440.69.2018.I)

[123] Dz. U. poz. 1636

[124] Decyzja z 17.12.2018 r. (sygn. akt: ZSOŚS.440.23.2018)

[125] Por. sprawa zakończona decyzją wydana w kolejnym okresie sprawozdawczym z 11.01.2019 r. (sygn. akt: ZSOŚS.440.128.2018)

Kluczowe znaczenie dla oceny tego rodzaju skarg ma ocena, czy interes prawny skarżącego jest realny i rzeczywisty. W tym celu zawsze analizowany jest zamiar skarżącego, który wnioskuje o udostępnienie danych osobowych dla potrzeb postępowania sądowego. W szczególności ocenie podlega konkretny stan faktyczny oraz realność woli wszczęcia postępowania sądowego przez skarżącego. Niejednokrotnie żądania dotyczące udostępnienia danych osobowych funkcjonariuszy wykraczały poza niezbędne zakres informacji wymaganych do zainicjowania np. postępowania cywilnego.

W jednej z rozpatrywanych spraw doszło do naruszenia przepisów o ochronie danych osobowych przez komendanta Policji, który przekazał sądowi dane osobowe funkcjonariusza Policji bez podstawy prawnej. Sąd zwrócił się do właściwego komendanta Policji o doręczenie wezwania sądowego jednemu z funkcjonariuszy do stawienia się na rozprawie w charakterze świadka. Taki sposób przesyłania doręczeń jest przewidziany w art. 134 § 1 ustawy z dnia 6 czerwca 1997 r., Kodeks postępowania karnego[126]. Natomiast komendant Policji, w odpowiedzi przekazał sądowi kserokopie zwolnień lekarskich tego funkcjonariusza oraz jego adres do korespondencji. Prezes UODO uznał takie działanie komendanta Policji za niezgodne z treścią przepisów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. W szczególności podstawy do takiego działania nie dawała komendantowi Policji treść art. 15 § 2 k.p.k., zgodnie z którym organy udzielają pomocy do przeprowadzenia postępowania w terminie określonym przez sąd. Natomiast stosownie do art. 15 § 1 k.p.k., Policja i inne organy w zakresie postępowania karnego wykonują polecenia sądu, referendarza sądowego i prokuratora oraz prowadzą pod nadzorem prokuratora śledztwo lub dochodzenie w granicach określonych w ustawie. Jednakże organ zobowiązany do przekazania wezwania do stawienia się na rozprawę zgodnie z art. 134 § 1 k.p.k. (tzw. doręczenie zastępcze) nie może przenosić ciążącego na nim obowiązku na sąd, przesyłając sądowi dane adresowe świadka, którym w przedmiotowej sprawie miał być wskazany funkcjonariusz Policji. Błędnym było również założenie, że można przekazać jakiekolwiek dane do bezpośredniego kontaktu organu ze świadkiem, czy też jakiekolwiek inne dane, o które wprost sąd nie występował.

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

Celem czynności kontrolnych jest ustalenie, czy jednostka kontrolowana przetwarza dane zgodnie z przepisami o ochronie danych osobowych. Szerokie uprawnienia kontrolerów UODO zostały odrębnie uregulowane w rozdziale 9 ustawy z 10 maja 2018 r. o ochronie danych osobowych zatytułowanym kontrola przestrzegania przepisów o ochronie danych osobowych. Postępowanie kontrolne ma odrębny charakter od postępowań administracyjnych prowadzonych przez Prezesa UDOO, w tym postępowań w sprawie naruszenia przepisów o ochronie danych osobowych. Do 24 maja 2018 r. czynności kontrolne były prowadzone zgodnie z przepisami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, a w zakresie w niej nie uregulowanym zgodnie z przepisami k.p.a. Aktualne przepisy wzmacniają kompetencje kontrolerów UODO.

Od 1 stycznia do 24 maja 2018 r. przeprowadzono łącznie 40 kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych oraz zwrócono się do administratora bezpieczeństwa informacji w jednym z podmiotów o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania. Od 25 maja 2018 roku do 31 grudnia 2018 r. kontrolerze UODO przeprowadzili łącznie 32 kontrole przestrzegania przepisów o ochronie danych osobowych.

Kontrole prowadzone w okresie od 1 stycznia do 24 maja 2018 r.

[126] Tj. Dz. U. z 2018 poz. 1987 – dalej jako k.p.a.

W okresie sprawozdawczym kontrolami prowadzonymi przez inspektorów Biura GIODO objęto w szczególności przetwarzanie danych osobowych przez uprawnione podmioty w związku z dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych VIS oraz dokonywania wglądu do danych SIS i VIS, zgodnie z przepisami ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[127]. Kontrole przeprowadzone zostały w wydziałach (referatach) konsularnych przy ambasadach Rzeczypospolitej Polskiej oraz urzędach celno-skarbowych.

W wyniku kontroli przeprowadzonych w ambasadach Rzeczypospolitej Polskiej ustalono, że dostęp danych VIS posiadają wyłącznie konsulowie, a więc osoby uprawnione w świetle przepisów ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. W wybranych urzędach celno-skarbowych badano przetwarzanie danych osobowych w związku z dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów oraz wglądu do danych SIS.

W toku przeprowadzonych kontroli nie stwierdzono uchybień, które stanowiłyby podstawę do zastosowania art. 18 ust. 1 pkt 1 ustawy, tj. nakazania przez Generalnego Inspektora w drodze decyzji administracyjnej przywrócenia stanu zgodnego z prawem, a w szczególności usunięcie uchybień.

Ponadto w trakcie ww. kontroli ustalono, że w urzędach celno-skarbowych są dokonywane sprawdzenia w Systemie Informacyjnym Schengen na wniosek naczelników urzędów skarbowych właściwych w sprawach podatku akcyzowego w celu weryfikacji pojazdów (badania legalności pochodzenia samochodów osobowych z tytułu nabycia wewnątrzwspólnotowego). Jednakże kwestia podstawy prawnej dokonywania sprawdzeń w Systemie Informacyjnego Schengen na wniosek naczelników urzędów skarbowych właściwych w sprawach podatku akcyzowego w celu weryfikacji pojazdów (badania legalności pochodzenia samochodów osobowych z tytułu nabycia wewnątrzwspólnotowego) wzbudziła wątpliwości GIODO, gdyż zgodnie z przepisami zarządzenia Ministra Rozwoju i Finansów z dnia 1 marca 2017 r. w sprawie organizacji jednostek organizacyjnych Krajowej Administracji Skarbowej oraz nadania im statutów[128], organami prowadzącym postepowania podatkowe w zakresie akcyzy są naczelnicy urzędów skarbowych, zatem nie jest to zadanie Służby Celno-Skarbowej. Należało bowiem rozważyć, czy takie sprawdzenia stanowią realizację określonych w przepisach ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym uprawnień Służby Celno-Skarbowej. Wobec powyższego GIODO na podstawie art. 19a ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych zwrócił się do Ministra Finansów o rozważenie, czy rzeczywiście w związku z postępowaniami prowadzonymi przez urzędy skarbowe istnieje konieczność dokonywania takich sprawdzeń, a jeżeli tak, to czy wymienione przepisy nie powinny zostać uzupełnione w taki sposób, aby urzędom skarbowym stworzyć możliwość dostępu do KSI i podjęcie w tym zakresie inicjatywy ustawodawczej.

W związku z wystąpieniem GIODO Minister Finansów poinformował o podjętych działaniach zmierzających do dokonania odpowiednich zmian legislacyjnych mających na celu umożliwienie korzystania z systemu SIS także przez naczelników urzędów skarbowych. Zmiany w ustawie o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym umożliwiające naczelnikom urzędów skarbowych dokonywanie weryfikacji pojazdów w systemie SIS wprowadzone zostały ustawą z dnia 9 listopada 2018 r. o zmianie ustawy o Krajowej Administracji Skarbowej oraz niektórych innych ustaw[129].

Ponadto we wskazanym okresie przeprowadzono także m.in. kontrole w podmiotach realizujących usługi finansowe. W wyniku tych kontroli ustalono, że pozyskują one kopie dokumentów tożsamości klientów. Ustalono również, że w przypadku wielu kopii dokumentów tożsamości dane

[127] Tj. Dz. U. z 2018 r. poz. 2162 ze zm.
[128] Dz. Urz. MRiF z 2017 r. poz. 41, z późn. zm.
[129] Dz. U. z 2018 r. poz. 2354

osobowe w nich przetwarzane nie zostały zanonimizowane w zakresie niektórych danych, tak aby pozyskać jedynie informacje niezbędne do ustalenia tożsamości klienta. W konsekwencji kontrolowane podmioty, zbierając od klientów kopie dokumentów tożsamości, pozyskiwały dane tych osób w zakresie szerszym (np. nazwisko rodowe, imiona rodziców, wizerunek, wzrost i kolor oczu), niż to było niezbędne do osiągnięcia celu przetwarzania danych, tj. potwierdzenia tożsamości klientów. W zakresie stwierdzonych uchybień wobec powyższych podmiotów wszczęte zostały postępowania administracyjne. Po otrzymaniu zawiadomień o wszczęciu postępowań administracyjnych kontrolowane podmioty usunęły uchybienia i dlatego GIODO wydał decyzje umarzające postępowania w ww. sprawach.

Kontrole prowadzone w okresie od 25 maja do 31 grudnia 2018 r.

Kontrole prowadzone przez kontrolerów UODO zostały przeprowadzone m.in. w zakresie: prowadzenia i zabezpieczenia rejestru mieszkańców, miejskiego monitoringu wizyjnego i przetwarzania danych w ramach platformy ePUAP.

Czynnościami kontrolnymi objęto także: brokerów danych, firmy windykacyjne, instytucje finansowe, serwisy internetowe, stowarzyszenia, a także spółdzielnie i wspólnoty mieszkaniowe, w tym w zakresie stosowania przez nie monitoringu wizyjnego, oraz działalność firm zajmujących się telemarketingiem.

Kontrole doraźne dotyczyły wtórnego przetwarzania danych osobowych pozyskanych ze źródeł powszechnie dostępnych bądź zakupionych baz danych oraz naruszeń ochrony danych polegających na uzyskaniu nieuprawnionego dostępu bądź niezamierzonej publikacji danych.

Impulsem do przeprowadzenia kontroli doraźnych były licznie napływające skargi (szczególnie w zakresie spełnienia obowiązku informacyjnego oraz wykonania praw osób, których dane dotyczą), zgłoszenia naruszeń ochrony danych osobowych przesłane przez administratorów oraz naruszenia zasygnalizowane w skargach.

Prowadzenie i zabezpieczenie rejestru mieszkańców

Zgodnie z planem kontroli sektorowych na rok 2018 kontrolerzy UODO przeprowadzili kontrole w pięciu jednostkach samorządu terytorialnego. Zakresem kontroli objęto sposób prowadzenia i zabezpieczenia rejestru mieszkańców przez kontrolowane podmioty. Celem przeprowadzonej kontroli było ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez wybrane podmioty.

Czynności kontrolne przeprowadzone zostały w okresie od sierpnia do grudnia 2018 r. Podstawę prawną przetwarzania danych przez wójta (burmistrza, prezydenta miasta) w związku z prowadzeniem rejestru mieszkańców stanowią przepisy ustawy o ewidencji ludności. Zgodnie z ówczesnym art. 6 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności[130], rejestr mieszkańców był prowadzony zgodnie z właściwością miejscową przez wójta (burmistrza, prezydenta miasta), zwanego dalej „organem gminy". Podczas kontroli oceniany był sposób prowadzenia i zabezpieczenia rejestru mieszkańców przez kontrolowane podmioty na podstawie obowiązującego w okresie kontroli stanu prawnego.

Aktualnie obowiązują znowelizowane przepisy ustawy o ewidencji ludności. Rejestr mieszkańców w podmiotach kontrolowanych prowadzony jest w systemach informatycznych o nazwie SELWIN lub OTAGO. Dane do rejestru mieszkańców są przekazywane w sposób automatyczny z rejestru PESEL. Natomiast rejestracji danych w rejestrze PESEL dokonują podmioty wymienione w art. 10 ustawy o ewidencji ludności. Wójt (burmistrz, prezydent miasta) jest organem właściwym w przypadku dokonywania zameldowania na pobyt stały lub czasowy (wprowadzane są wówczas dane w zakresie określonym w art. 8 pkt 14–21 ustawy o ewidencji ludności), w przypadku dokonywania zameldowania na pobyt stały i czasowy cudzoziemca (wprowadzane są wówczas dane w zakresie

[130] Dz. U. z 2018 r. poz. 1382

określonym w art. 8 pkt 1, 3–7, 9–21, 24, 24a i 26 ustawy o ewidencji ludności), w przypadku wydania dowodu osobistego (wprowadzane są dane, o których mowa w art. 8 pkt 22 ustawy o ewidencji ludności) oraz w przypadku złożenia wniosku o nadanie numeru PESEL (wprowadzane są wówczas dane w zakresie określonym w art. 8 pkt 1–13, 15 i 22–24 ustawy o ewidencji ludności).

Podstawą do wprowadzenia danych przez wójta (burmistrza, prezydenta miasta) do rejestru PESEL w zakresie określonym w powołanych wyżej przepisach ustawy o ewidencji ludności są składane przez mieszkańców gminy zgłoszenia pobytu stałego, zgłoszenia pobytu czasowego, zgłoszenia wymeldowania z miejsca pobytu stałego, zgłoszenia wymeldowania z miejsca pobytu czasowego, zgłoszenia wyjazdu poza granicę Rzeczypospolitej Polskiej, zgłoszenia powrotu z wyjazdu poza granicę Rzeczypospolitej Polskiej trwającego dłużej niż sześć miesięcy.

Na podstawie dokonanych przez kontrolerów UODO ustaleń należy stwierdzić, że wymiana danych odbywała się w dużej mierze w sposób zgodny z wymogami wynikającymi z przepisów o ochronie danych oraz przepisów ustawy o ewidencji ludności. Stwierdzone w toku kontroli uchybienia dotyczące klauzuli informacyjnej odnotowane zostały w 5 kontrolowanych jednostkach samorządu terytorialnego. Polegały ono na tym, że klauzula informacyjna nie zawierała kompletnych informacji dotyczących poszczególnych administratorów, w szczególności w zakresie celu przetwarzania i podstawy prawnej, odbiorców danych, okresu przechowywania danych. Ponadto w klauzuli nie zostały zawarte informacje o wszystkich odbiorcach danych, w szczególności o podmiocie zobowiązanym do serwisu eksploatacyjnego oprogramowania komputerowego SELWIN, a także o stronach i uczestnikach postępowań administracyjnych w sprawach meldunkowych. Ponadto klauzula nie zawierała informacji o okresie przechowywania danych osobowych przetwarzanych przez administratora w związku z prowadzonym rejestrem mieszkańców. Klauzula informacyjna w części dotyczącej informacji o dowolności lub obowiązku podania danych zawierała wyłącznie informację, że podanie danych wynika z ustawy o ewidencji ludności, natomiast nie wskazuje konsekwencji niepodania danych. Ponadto określając cele przetwarzania danych, nie wskazano, które z tych celów są realizowane przez administratora[131].

Kolejne uchybienia dotyczyły umowy powierzenia przetwarzania danych osobowych w jednej z kontrolowanych jednostek samorządu terytorialnego. Polegały one na tym, że zawarta umowa
na usługę asysty technicznej i konserwacji oprogramowania użytkowego Zintegrowanego Systemu Wspomagania Zarządzania Miastem (System OTAGO) w zakresie odnoszącym się do danych osobowych nie zawierała informacji określonych w art. 28 ust. 3 lit. e), f), h) RODO, tj. zobowiązania podmiotu przetwarzającego do wspierania administratora w wypełnianiu jego obowiązków wynikających z ogólnego rozporządzenia o ochronie danych[132].

W dwóch kontrolowanych jednostkach naruszona została zasada integralności i poufności. Stwierdzone naruszenia polegały na tym, że w pomieszczeniach obsługi interesantów stanowiska o wydanie dowodu osobistego oraz stanowiska dla osób dopełniających obowiązku meldunkowego nie zostały od siebie oddzielone przegrodami, które uniemożliwiłyby zapoznanie się z danymi osoby obsługiwanej przy sąsiednim stanowisku, co umożliwiało naruszenie poufności przetwarzanych danych osobowych[133].

W 5 kontrolowanych jednostkach samorządu terytorialnego stwierdzono uchybienia dotyczące rejestru czynności przetwarzania danych, które polegały na tym, że w rejestrze czynności nie została ujęta informacja o wszystkich odbiorcach danych przetwarzanych w związku z prowadzeniem rejestru mieszkańców, w tym o stronach i uczestnikach postępowań administracyjnych prowadzonych w sprawach meldunkowych. Ponadto w rejestrze ujęte zostały

[131] ZSPU.421.1.2018,ZSPU.421.2.2018, ZSPU.421.7.2018, ZSPU.421.8.2018, ZSPU.421.10.2018
[132] kontrola: ZSPU.421.2.2018
[133] ZSPU.421.2.2018, ZSPU.421.7.2018

odrębnie czynności przetwarzania związane z obowiązkiem meldunkowym prowadzone w formie dokumentacji papierowej oraz w sposób elektroniczny. Planowany termin usunięcia danych został określony dla formy papierowej jako :„zgodnie z kategorią archiwalną", a dla formy elektronicznej – „bezterminowo". Określona w ten sposób retencja danych osobowych przetwarzanych w tym samym celu, a jedynie za pomocą innego narzędzia, nie jest spójna. Ponadto zgodnie z art. 30 ust. 1 lit. f) RODO należy w rejestrze wskazać konkretny termin, w którym administrator planuje usunąć dane[134].

W jednej z kontrolowanych jednostek samorządu terytorialnego stwierdzono naruszenia dotyczące udostępniania dokumentacji z archiwum zakładowego. Administrator nie wdrożył wystarczających środków organizacyjnych mających na celu zapewnienie odpowiedniego bezpieczeństwa udostępnianych danych, ponieważ nie ma on możliwości ustalenia, komu, w jakim zakresie oraz w jakim czasie udostępnione zostały dane osobowe przechowywane w archiwum zakładowym, co stanowi naruszenie art. 5 ust. 1 lit. f) oraz art. 24 ust. 1 ogólnego rozporządzenia o ochronie danych[135].

W 2 kontrolowanych jednostkach samorządu terytorialnego[136] naruszono art. 5 ust. 1 lit. e) RODO w odniesieniu do przechowywania dokumentów związanych ze sprawami meldunkowymi przez okres dłuższy niż wskazany w rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[137].

W toku kontroli w jednej z kontrolowanych jednostek stwierdzono naruszenie art. 5 ust. 1 lit. e) ogólnego rozporządzenia o ochronie danych poprzez przetwarzanie danych osobowych zawartych w dokumentach potwierdzających tytuł prawny do lokalu przez okres dłuższy (załączniki zawierające dokumenty potwierdzające tytuł prawny do lokalu nie są z systemu usuwane), niż jest to niezbędne do celów, w jakich zostały przedłożone[138].

Ponadto, skierowane zostały do kontrolowanych podmiotów zalecenia dotyczące przeanalizowania przez administratora sposobu powierzenia zadań inspektorowi ochrony danych pod kątem powstania konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

Ponadto zalecono jednemu z kontrolowanych jednostek, aby w razie kontynuowania zlecania podmiotowi zewnętrznemu niszczenia dokumentów została zawarta umowa powierzenia przetwarzania danych osobowych, zawierająca elementy wymienione w art. 28 ust. 3 RODO.

Wobec 5 podmiotów, w których stwierdzono uchybienia dające podstawę do zastosowania przez Prezesa UODO środków, o których mowa w art. 58 ogólnego rozporządzenia o ochronie danych, wszczęte zostały postępowania administracyjne i wydane zostały 4 decyzje, w tym 1 decyzja umarzająca postępowanie w odniesieniu do nieprawidłowości usuniętych w toku prowadzonych postępowań oraz 3 decyzje nakazująco – umarzające.

Ponadto w związku z przeprowadzonymi kontrolami skierowane zostało wystąpienie do Ministerstwa Cyfryzacji zmierzające do zapewnienia prawidłowej realizacji obowiązku informacyjnego, o którym mowa w art. 13 ogólnego rozporządzenia o ochronie danych, względem osób spełniających obowiązek meldunkowy, poprzez ujęcie w klauzuli informacyjnej dotyczącej przetwarzania danych osobowych w związku z realizacją obowiązków wynikających z przepisów ustawy z dnia 24 września 2010 r. o ewidencji ludności[139] wszystkich informacji dotyczących przetwarzania danych przez każdego z administratorów wskazanych w tej klauzuli, a ponadto o przekazanie wójtom (burmistrzom, prezydentom miast) uzupełnionej o informacje wskazane w pkt 1) klauzuli informacyjnej, celem jej udostępniania osobom, których dane dotyczą, podczas

[134] kontrole: ZSPU.421.1.2018,ZSPU.421.2.2018, ZSPU.421.7.2018, ZSPU.421.8.2018, ZSPU.421.10.2018
[135] ZSPU.421.1.2018
[136] ZSPU.421.8.2018, ZSPU.421.10.2018
[137] Dz. U. Nr 14, poz. 67
[138] ZSPU.421.10.2018
[139] Dz.U z 2018 r. poz. 1382 z poźn. zm.

pozyskiwania danych osobowych przy realizacji przez wójtów (burmistrzów, prezydentów miast) czynności przetwarzania danych na podstawie ustawy z dnia 24 września 2010 r. o ewidencji ludności.

Ponadto zarówno Minister Cyfryzacji, jak i Minister Spraw Wewnętrznych i Administracji zostali poinformowani, że przedstawiona klauzula informacyjna nie zawiera pełnych informacji, które zgodnie z art. 12 ust. 1 ogólnego rozporządzenia o ochronie danych) mają zapewnić udzielenie osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 ogólnego rozporządzenia o ochronie danych, zgodnie z zasadą przejrzystej komunikacji. W szczególności w przesłanej klauzuli, w części dotyczącej odbiorców danych, nie ujęto stron i uczestników postępowań administracyjnych w sprawach o zameldowanie/wymeldowanie, a wśród podmiotów przetwarzających nie wskazano podmiotów świadczących usługi w zakresie utrzymania i serwisu systemu informatycznego służącego do prowadzenia rejestru mieszkańców przez wójta (burmistrza, prezydenta miasta). Ponadto określając okres przechowywania danych nie został podany konkretny termin usunięcia danych oraz nie wskazano skutków niepodania danych osobowych.

Zarówno Minister Cyfryzacji, jak i Minister Spraw Wewnętrznych i Administracji poinformowani zostali, że w związku z istotnymi zmianami w zakresie udostępniania danych z rejestru PESEL, może powstać konieczność dostosowania obecnie przyjętych wzorów klauzul informacyjnych do zmian wynikających ze znowelizowanych przepisów ustawy o ewidencji ludności.

Ponadto w związku z przeprowadzonymi kontrolami skierowane zostało wystąpienie do Ministerstwa Cyfryzacji zmierzające do podjęcia stosownych działań mających na celu wyeliminowanie praktyki nadawania upoważnień do przetwarzania danych osobowych zgromadzonych w rejestrze PESEL, o których mowa w art. 29 ogólnego rozporządzenia o ochronie danych, wójtom (burmistrzom, prezydentom miast), w przypadkach w których dostęp do ww. rejestru wynika z przepisów prawa.

Miejski monitoring wizyjny

Zgodnie z planem kontroli sektorowych na rok 2018 kontrolerzy UODO przeprowadzili kontrolę w 2 jednostkach samorządu terytorialnego w zakresie przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego. Podstawą prawną przetwarzania danych osobowych przez kontrolowane jednostki samorządu terytorialnego w ramach funkcjonującego w danym mieście systemu monitoringu wizyjnego jest art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym[140]. Zakres przetwarzanych danych osobowych obejmuje przede wszystkim wizerunek osób poruszających się po obszarze objętym monitoringiem. Kamery działające w ramach systemów miejskiego monitoringu wizyjnego objętych kontrolą nie posiadają lub nie mają aktywnej funkcjonalności rozpoznawania twarzy ani też możliwości śledzenia danej osoby. Ponadto kamery te nie rejestrują dźwięku.

Na podstawie dokonanych przez kontrolerów UODO ustaleń należy stwierdzić, że wymiana danych odbywała się w dużej mierze w sposób zgodny z wymogami wynikającymi z przepisów o ochronie danych osobowych oraz przepisów ustawy o samorządzie gminnym.

W obu kontrolowanych podmiotach stwierdzono uchybienia polegające na tym, że nie opracowały one ocena skutków dla ochrony danych, mimo że przetwarzanie danych osobowych wiąże się zarówno z operacjami znacznej ilości danych na szczeblu regionalnym (znaczna część miasta znajduje się pod obserwacją kamer), jak i może wpłynąć na dużą liczbę osób, ze względu na wielość osób zarejestrowanych przez kamery wchodzące w skład miejskiego monitoringu wizyjnego, a tym samym naruszony został art. 35 ust. 1 RODO[141]. Ponadto w opracowanej w podmiocie kontrolowanym dokumentacji analizy ryzyka nie zostały opisane działania naprawcze, a także nie przeprowadzono oceny ryzyka dla poszczególnych zagrożeń, mimo że przetwarzanie danych

[140] Dz. U. z 2018 r. poz. 994 z późn. zm.

[141] ZSPU.421.6.2018, ZSPU.421.9.2018 Dz. U. z 2018 r. poz. 994 z późn. zm.

[141] ZSPU.421.6.2018, ZSPU.421.9.2018

osobowych wiązało się zarówno z operacjami znacznej ilości danych na szczeblu regionalnym (znaczna część miasta znajduje się pod obserwacją kamer), jak i mogło wpłynąć na dużą liczbę osób, ze względu na wielość osób zarejestrowanych przez kamery wchodzące w skład miejskiego monitoringu wizyjnego przez co naruszone zostały przepisy art. 24 ust. 1 i art. 32 ust. 1 ogólnego rozporządzenia o ochronie danych.

Ponadto, nie zamieszczono klauzul informacyjnych przy niektórych punktach kamerowych. Brakowało także piktogramów. Informacje tego typu powinny zostać umieszczone odpowiednio w obszarze, obiekcie czy innym miejscu objętym monitoringiem miejskim. Co więcej, w klauzulach informacyjnych dotyczących przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego nie została w sposób prawidłowy wskazana podstawa prawna przetwarzania danych, w nieprawidłowy sposób określone zostały cele, dla których monitoring jest stosowany, brak było informacji kontaktowych inspektora ochrony danych. W klauzuli informacyjnej nie został także wymieniony pełen katalog praw, z których skorzystać mogą osoby zarejestrowane przez system monitoringu miejskiego. Natomiast w innym kontrolowanym podmiocie w klauzuli informacyjnej dotyczącej miejskiego monitoringu wizyjnego, wymienione zostały prawa, które nie przysługują osobom, których dane dotyczą.

W toku kontroli stwierdzono powierzenie w jednej z kontrolowanych jednostek zadań inspektorowi ochrony danych osobie zatrudnionej na stanowisku sekretarza miasta co powodowało konflikt interesów, o którym mowa w art. 38 ust. 6 ogólnego rozporządzenia o ochronie danych[142].

Ponadto skierowane zostały do kontrolowanych podmiotów zalecenia dotyczące zweryfikowania przez administratora, upoważnień do przetwarzania danych osobowych, pod kątem prawidłowego oznaczenia osób, którym nadanie przedmiotowych upoważnień jest niezbędne w związku z wykonywanymi zadaniami służbowymi, a także skorygowanie opisów stanowisk w taki sposób, żeby szczegółowo i precyzyjnie odnosiły się do czynności związanych z przetwarzaniem danych osobowych.

Co więcej, skierowane zostały do kontrolowanych podmiotów zalecenia dotyczące zweryfikowania przez administratora, upoważnień do przetwarzania danych osobowych. Przyśpieszenia procesu wymiany upoważnień do przetwarzania danych osobowych na upoważnienia dostosowane do wymogów wynikających z przepisów ogólnego rozporządzenia o ochronie danych osobowych. Zalecono także, aby z nadaniem nowych upoważnień do przetwarzania danych osobowych opracowano ewidencję osób upoważnionych do przetwarzania danych osobowych. W nowych upoważnieniach powinny być określone nie tylko zbiory danych osobowych, do których ma dostęp upoważniana osoba, ale także zakres operacji, które taka osoba może wykonywać na danych osobowych w danym zbiorze danych.

Ponadto skierowane zostało do kontrolowanego podmiotu zalecenie dotyczące tego, że w klauzuli informacyjnej, opracowanej dla monitoringu wizyjnego w zakresie nagrywanych sesji rady miasta, użyto sformułowania, że nagrania te będą zamieszczane na stronie BIP bezterminowo, administrator powinien wdrożyć odpowiednie procedury usunięcia, okresu retencji i ochrony danych osobowych, przetwarzanych w ramach rejestrowanych i udostępnianych na stronie BIP sesji rady miasta, przy czym pożądanym działaniem byłoby również podjęcie działań w celu rozdzielenia nagrywanych ww. sesji od miejskiego monitoringu wizyjnego.

Co więcej, skierowane zostało do kontrolowanego podmiotu zalecenie dotyczące umów zawartych z innymi podmiotami, na podstawie których możliwe byłoby wykorzystanie ich infrastruktury (kamer) i które poprzedzone powinno być rzetelnie przeprowadzoną analizą ryzyka przetwarzania danych osobowych oraz oceną skutków. Wówczas administrator danych zebranych w związku z funkcjonującym systemem miejskiego monitoringu wizyjnego powinien podjąć decyzję o konieczności i formie zawarcia porozumienia z tymi podmiotami. W zależności od wybranego rodzaju

[142] ZSPU.421.6.2018

umowy powinna ona spełniać wymogi określone w art. 26 lub 28 ogólnego rozporządzenia o ochronie danych.

Ponadto skierowane zostały do kontrolowanych podmiotów zalecenia dotyczące wspólnych uzgodnień pomiędzy prezydentem miasta i komendantem straży miejskiej w sprawie przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego, których powinni dokonać, jako współadministratorzy tych danych. Pisemne porozumienie zawarte pomiędzy stronami powinno uwzględniać fakt, że straż miejska stosuje przepisy ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości do przetwarzania danych osobowych w tych przypadkach, gdy przetwarzanie to będzie następowało w celach wskazanych w art. 1 pkt 1 u.o.d.o.z.z.

Przetwarzanie danych w ramach platformy ePUAP

Kontrolerzy UODO przeprowadzili także kontrolę w dwóch podmiotach, w zakresie przetwarzania przez administratora danych osobowych w ramach platformy ePUAP, a w szczególności użytkowników tej platformy[143]. Celem kontroli było ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez wybrane podmioty. Dane osobowe przetwarzane w ramach platformy ePUAP, w tym dane osobowe użytkowników tej platformy są przetwarzane przez podmiot kontrolowany na podstawie art. 19a ust. 1 i 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne[144]. Osoba zainteresowana korzystaniem z platformy ePUAP musi założyć konto w ePUAP, zgodnie z § 3 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[145]. Podczas wypełniania formularza rejestracyjnego dostępnego na stronie internetowej epuap.gov.pl, należy podać dane wskazane w § 4 powołanego rozporządzenia, tj. imienia (imion), nazwiska, numer PESEL, adresu poczty elektronicznej (adres ten trzeba potwierdzić, wpisując go ponownie), numeru telefonu komórkowego, określeniem identyfikatora użytkownika. Założenie konta w ePUAP powoduje jednoczesne założenie konta profilu zaufanego.

W toku kontroli stwierdzono uchybienia dotyczące realizowania przez administratora obowiązku informacyjnego. Jednym z nich była kwestia informowania osób wskazanych do odbioru kluczy kryptograficznych (certyfikatów). Kontrolowany podmiot powoływał się na treść art. 14 ust. 5 lit. a) ogólnego rozporządzenia o ochronie danych, wskazując, że nie ciąży na nim obowiązek informacyjny wobec osób wskazanych do odbioru nośników kluczy kryptograficznych (certyfikatów), wymienionych we wniosku o wydanie certyfikatu dla systemu teleinformatycznego. Jednak administrator w żaden sposób nie wykazał, aby osoby wskazane do odbioru certyfikatów posiadały informacje określone w ust. 1–4 powołanego artykułu, w szczególności wymaganych informacji nie umieszczono w ramach opracowanej w dokumentacji wewnętrznej podmiotu kontrolowanego, czy też w innych dokumentach, z którymi mogą się zapoznać ww. osoby. W związku z powyższym, uznano, że administrator nie realizuje obowiązku informacyjnego, o którym mowa w art. 14 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych wobec osób wskazanych do odbioru nośników kluczy kryptograficznych.

Kolejnymi uchybieniami związanymi z realizacją obowiązku informacyjnego było niedostosowanie opracowanej klauzuli informacyjnej dla przetwarzania danych w ramach platformy ePUAP do treści art. 13 ust. 1 lit. a), c) i e) ogólnego rozporządzenia o ochronie danych. Uchybienia te polegały na nie wskazaniu informacji o odbiorcach danych, jak również na nieprawidłowym określeniu retencji danych w ramach platformy ePUAP. Dalsze naruszenia dotyczyły pominięcia wskazania w podstawie prawnej przetwarzania przesłanek przetwarzania danych

[143] Np. kontrola: ZSPU.421.4.2018

[144] Dz.U. 2005 nr 64 poz. 565.

[145] Dz. U. poz. 1626.

osobowych, określonych w art. 6 ust. 1 ogólnego rozporządzenia o ochronie danych, a także nie wskazania informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

Administrator określił również w sposób nieprawidłowy w rejestrze czynności przetwarzania opis kategorii osób, których dane dotyczą, jak również nie ujął w rejestrze, w sposób przejrzysty, informacji o planowanym terminie usunięcia danych osobowych, naruszając tym samym art. 30 ust. 1 lit. c) i f) ogólnego rozporządzenia o ochronie danych, co stanowiło kolejne stwierdzone przez kontrolerów uchybienie.

W toku dokonanych czynności kontrolnych ustalono, że podczas procesu zakładania konta profilu zaufanego użytkownik jako jedną z danych podaje adres poczty elektronicznej. O założeniu konta w ePUAP i konta profilu zaufanego użytkownik powiadamiany jest za pomocą wiadomości przesłanej na podany w treści formularza rejestracyjnego adres poczty elektronicznej. Przesłana wiadomość nie wymaga podjęcia przez użytkownika żadnej czynności w celu potwierdzenia poprawności podanego adresu elektronicznego. Tym samym uznano, że administrator, wobec zagrożenia jakim jest ryzyko przejęcia konta profilu zaufanego wobec braku ww. weryfikacji adresu e-mail na etapie rejestrowania oraz odzyskiwania dostępu do konta, nie wdrożył odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Naruszono tym samym przepisy art. 24 ust. 1 i art. 32 ust. 1 ogólnego rozporządzenia o ochronie danych.

Przeprowadzone kontrole doprowadziły ponadto do sformułowania zaleceń dla podmiotu kontrolowanego. Zalecenia te odnosiły się m.in. do kwestii prawidłowego sporządzania i wydawania upoważnień do przetwarzania danych dla poszczególnych pracowników jednostki a także zgłaszania naruszeń ochrony danych oraz ich dokumentowania w dedykowanym do tego celu rejestrze, zgodnie z art. 33 ogólnego rozporządzenia o ochronie danych.

Na skutek dokonanych czynności kontrolnych, w podmiotach kontrolowanych podjęto szereg działań naprawczych, w tym opracowano klauzulę informacyjną dotyczącą przetwarzania danych osobowych, zgodnie z treścią art. 14 ogólnego rozporządzenia o ochronie danych, dedykowaną osobom upoważnionym do odbioru kluczy kryptograficznych. Zmodyfikowano również klauzule informacyjne dla użytkowników platformy ePUAP, dostępne na stronach internetowych epuap.gov.pl i pz.gov.pl, poprzez wskazanie podstawy prawnej, odbiorców danych oraz okresu przechowywania danych.

W ramach działań podmiotu kontrolowanego uzupełniony został ponadto rejestr czynności przetwarzania prowadzony przez administratora w zakresie wskazanych w zawiadomieniu o wszczęciu postępowania administracyjnego uchybień, jak również dokonano modyfikacji formularza rejestracji użytkownika, dostępnego na stronie internetowej profilu zaufanego, poprzez dodanie pola umożliwiającego ponowne wprowadzenie adresu e-mail, co jednocześnie wymusza weryfikację ww. adresu wobec konieczności jego dwukrotnego podania.

Spółdzielnie oraz wspólnoty mieszkaniowe

Kontrole zostały przeprowadzone w dwóch spółdzielniach mieszkaniowych oraz w jednej wspólnocie mieszkaniowej. Zakresem kontroli objęto przetwarzanie danych osobowych utrwalonych przy użyciu elektronicznych urządzeń rejestrujących obraz oraz dźwięk, tj. za pomocą systemu monitoringu wizyjnego. Czynności kontrolne przeprowadzone w jednej ze spółdzielni mieszkaniowej wykazały, że jedna z kamer systemu monitoringu zainstalowana jest na półpiętrze klatki schodowej. Kamera ta swym zasięgiem obejmuje drzwi wejściowe do dwóch lokali mieszkalnych położonych na dwóch kondygnacjach klatki schodowej. W wyniku kontroli ustalono, że decyzja o zamontowaniu przedmiotowej kamery, została podjęta przez zarząd spółdzielni, w związku z licznymi skargami jakie wpływały do spółdzielni od dwóch sąsiadów mieszkających w tej klatce schodowej. Skargi te dotyczyły dewastacji mienia spółdzielni oraz o zakłócania porządku domowego. Z analizy zebranego

materiału wynika, że jedna ze skarżących zarzuca zarządowi spółdzielni, że stałe monitorowanie drzwi wejściowych do jej lokalu mieszkalnego, narusza jej prywatność oraz prawo do ochrony jej wizerunku oraz wizerunku innych osób (osób które ją odwiedzają). W odczuciu skarżącej stosowanie monitoringu powoduje naruszenie jej życia prywatnego i rodzinnego, bowiem świadomość, że ciągle jest obserwowana ogranicza jej swobodę i wzbudza zaniepokojenie. Oceniając zebrany materiał dowodowy, stwierdzono, że sposób zamontowania przedmiotowej kamery narusza przepisy prawa, jak również obowiązujące w spółdzielni zasady funkcjonowania monitoringu wizyjnego. Na tej podstawie stwierdzono, że spółdzielnia w ww. zakresie narusza postanowienia art. 6 ust. 1 pkt f ogólnego rozporządzenia o ochronie danych, zgodnie z którym przetwarzanie jest zgodne z prawem, gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

Ponadto objęte kontrolą spółdzielnie nie wyznaczyły inspektora ochrony danych. W ich ocenie przesłanki, o których mowa w art. 37 ust. 1 lit. a, b i c ogólnego rozporządzenia o ochronie danych nie mają w stosunku do nich zastosowania, bowiem spółdzielnie mieszkaniowe nie są organem lub podmiotem publicznym oraz nie przetwarzają danych osobowych na tzw. dużą skalę. Nie ulega wątpliwości, że przesłanka, o której mowa w art. 37 ust. 1 lit. a nie dotyczy spółdzielni mieszkaniowych, bowiem faktycznie nie są one organem lub podmiotem publicznym. Natomiast odnosząc się do pozostałych przesłanek, o których mowa w art. 37 ust. 1 lit. b i lit. c. ogólnego rozporządzenia o ochronie danych, wskazać należy, że w związku ze stosowaniem monitoringu spółdzielnie wykonują regularne operacje na danych, które polegają np. na: zapisywaniu, przeglądaniu, udostępnianiu i usuwaniu nagrań zarejestrowanych zdarzeń i osób. A tym samym uznać należy, że stosowanie monitoringu przez spółdzielnie wymaga regularnego i systematycznego monitorowania osób na tzw. dużą skalę.

Ponadto istotną kwestią jest również to, że spółdzielnie w związku ze stosowaniem monitoringu przetwarzają dane osobowe (wizerunek), nie tylko samych lokatorów tych spółdzielni, lecz także innych osób, np. osób odwiedzających mieszkańców osiedli spółdzielni, osób prowadzących i korzystających z punktów usługowo-handlowych zlokalizowanych na terenie tych spółdzielni. Na tej podstawie w ocenie Prezesa UODO spółdzielnie te są zobowiązane do wyznaczenia inspektora ochrony danych. Postępowania w tych sprawach są w toku.

Telemarketing

Czynności kontrolne zostały przeprowadzone w podmiocie, który prowadzi telemarketing na rzecz innych podmiotów. W tym celu podmiot ten, w trakcie prowadzonych rozmów telefonicznych pozyskuje informacje o osobach zainteresowanych udziałem w spotkaniach, na których prezentowane są produkty i usługi innych podmiotów.

W toku kontroli ustalono, że podmiot kontrolowany nie posiada baz danych zawierających numery telefonów, na które wykonywane są połączenia telefoniczne. Do wykonywania tej działalności podmiot kontrolowany wykorzystuje system informatyczny dostarczony przez podmiot mający siedzibę w innym państwie Unii Europejskiej. W toku kontroli ustalono, że konsultant telefoniczny nie wybiera danego numeru telefonu, a system informatyczny automatycznie wykonuje połączenie z danym numerem telefonu (stacjonarnym lub komórkowym). Konsultant nie posiada dostępu do informacji o wybranym numerze telefonu (ani w trakcie łączenia z danym numerem ani też po połączeniu). Funkcjonalność tego systemu nie uniemożliwia dostępu do informacji o wybranym numerze telefonu. Informacja o takim ograniczeniu zapisana jest w umowie na korzystanie z tego systemu.

W celu ustalenia legalności przetwarzanych danych osobowych w tym systemie, podstaw prawnych na podstawie, których za pomocą tego systemu następuje przekazywanie/udostępnianie danych innym podmiotom oraz ustalenia jakie podmioty korzystają z tego systemu oraz wyjaśnienie

kwestii, kto jest administratorem danych osobowych przetwarzanych w tym systemie i ustalenia, czy w związku z przetwarzaniem danych osobowych za pomocą tego systemu zostały zawarte umowy o powierzeniu przetwarzania danych, Prezes UODO wystąpił do organu nadzorczego kraju, w którym siedzibę posiada podmiot będący dostawcą przedmiotowego systemu informatycznego. Dopiero otrzymane wyniki dokonanych ustaleń (w zakresie, o którym mowa powyżej) pozwolą na ocenę procesu przetwarzania danych osobowych przez podmiot kontrolowany.

Brokerzy danych

Kontrola przeprowadzona została w jednym z podmiotów zajmującym się wtórnym przetwarzaniem danych osobowych pozyskanych ze źródeł powszechnie dostępnych – rejestrów publicznych, dotyczyła wypełnienia przez administratora obowiązku informacyjnego wynikającego z art. 14 ust. 1 rozporządzenia 2016/679.

W toku kontroli ustalono, że spółka przetwarza dane osobowe m.in. osób fizycznych prowadzących działalność gospodarczą, które zostały pozyskane z rejestrów publicznych – Centralnej Ewidencji i Informacji o Działalności Gospodarczej, Monitora Sądowego i Gospodarczego oraz tych, które prowadzi Główny Urząd Statystyczny. Spółka wypełniła obowiązek informacyjny, wysyłając informację na wszystkie adresy poczty elektronicznej posiadane w swojej bazie danych oraz zamieściła klauzulę informacyjną na swojej stronie internetowej. Spółka podjęła decyzję, aby m.in. ze względu na koszty nie realizować obowiązku informacyjnego poprzez wysłanie widomości SMS do osób, do których nie posiadała adresu e-mail, nie zdecydowała się również na spełnienie obowiązku informacyjnego poprzez wysłanie tradycyjnej korespondencji do osób fizycznych prowadzących działalność gospodarczą ze względu na koszty.

W związku z powyższym wszczęto wobec Spółki postępowanie administracyjne w zakresie naruszenia art. 14 ust. 1 rozporządzenia. W przedmiotowej sprawie w roku 2019 wydano decyzję administracyjną, nakazującą spełnienie obowiązku informacyjnego oraz nakładającą administracyjną karę pieniężną.

Firmy windykacyjne oraz instytucje finansowe

Kontrolerzy UODO przeprowadzili także dwie kontrole doraźne w firmach windykacyjnych. Przeprowadzenie kontroli zainicjowane było licznie napływającymi skargami w szczególności w związku z prowadzeniem tzw. „giełd wierzytelności" oraz publikacją danych dłużników. Zakresem kontroli objęto w szczególności zbadanie legalności przetwarzanych danych.

Jak ustalono w toku jednej z kontroli przedsiębiorcy zajmujący się obrotem wierzytelnościami/dochodzący swojej wierzytelności może co do zasady podawać do publicznej wiadomości dane osobowe dłużników w celu sprzedaży wierzytelności. Jest to bowiem konieczne do określenia danej wierzytelności wystawionej na sprzedaż, a działanie takie znajduje oparcie w art. 6 ust. 1 pkt f RODO (przed 25 maja 2018 r. działanie takie znajdowało podstawę w art. 23 ust. 1 pkt 5 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych). W przypadku oświadczenia woli zawarcia umowy sprzedaży wierzytelności bezsporne jest, że wierzytelność tę należy skonkretyzować. Dostateczne oznaczenie wierzytelności jest niezbędnym warunkiem, aby mogła ona stać się przedmiotem, którym można rozporządzić. Każdy dłużnik musi zatem liczyć się z tym, że popadając w zwłokę w spełnieniu zobowiązania, jego prawo do prywatności może zostać ograniczone ze względu na dochodzenie przez wierzyciela należnych kwot. Uzasadnione jest jednak takie wskazanie danych osobowych dłużnika, które są tylko niezbędne do określenia tej wierzytelności. Zgodnie bowiem z zasadą „minimalizacji danych" wyrażoną w art. 5 ust. 1 pkt c) RODO powinny być udostępniane tylko te dane, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

W związku z licznie napływającymi sygnałami dotyczącymi nieprawidłowości w procesie przetwarzania danych przeprowadzono kontrole doraźną w firmie zajmującej się udzielaniem pożyczek tzw. „chwilówek". Zakresem kontroli objęto zakres przetwarzanych danych pozyskanych

w celu zawarcia umowy, wypełnienie przez administratora obowiązku informacyjnego oraz żądań osób, których dane dotyczą w szczególności żądania usunięcia danych.

Krwiolecznictwo

Kontrolę dotyczącą sektora zdrowia, przeprowadzono w jednym z regionalnych centrów krwiodawstwa i krwiolecznictwa. Zakresem kontroli objęto przetwarzanie regionalnych centrów krwiodawstwa i krwiolecznictwa danych osobowych dawców krwi w ramach stacjonarnych i mobilnych punktów poboru krwi.

W toku kontroli badano m.in. zakres, cel i rodzaj przetwarzanych danych osobowych dawców krwi, weryfikowano także sposób wypełnienia obowiązków administratora danych, wynikających z RODO, w tym wdrożenie odpowiednich środków technicznych i organizacyjnych, celem zapewnienia, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO, oraz z uwzględnieniem ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 24 i art. 32 RODO).

Oświata

Prowadzono także kontrole w placówkach oświatowych, w których kontrolowano przetwarzanie danych osobowych uzyskanych za pośrednictwem środków technicznych umożliwiających rejestrację obrazu (monitoring wizyjny).

W toku powyższych kontroli weryfikacji poddano m.in. podstawę prawną przetwarzania danych osobowych uzyskanych w wyniku monitoringu, zakres i rodzaj przetwarzanych danych osobowych oraz cel ich przetwarzania, a także okres przez jaki są one przetwarzane. Upoważnieni pracownicy organu sprawdzili także czy administratorzy dokumentują wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (art. 33 ust. 5 RODO). Jedna z prowadzonych kontroli obejmowała dodatkowo zabezpieczenie danych osobowych uczniów oraz ich rodziców lub opiekunów prawnych przetwarzanych w zapisie papierowym.

W opisywanym roku sprawozdawczym przeprowadzono także kontrolę w publicznej szkole podstawowej z oddziałami integracyjnymi. Przedmiotem kontroli było zbadanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych, w zakresie przetwarzania przez szkołę danych osobowych za pomocą udostępnianej przez wydawnictwo platformy internetowej, na której znajdują się m.in. elektroniczne wersje podręczników, z których korzystają uczniowie szkoły.

W toku kontroli zbadano m.in. podstawę prawną przetwarzania danych osobowych oraz źródła ich pozyskania, a także zakres, cel i rodzaj przetwarzanych danych osobowych. Ponadto weryfikacji poddany został sposób zbierania i udostępniania danych osobowych. Organ weryfikował także sposób dopełnienia obowiązków administratora wynikających z art. 12, art. 13 ust. 1 i ust. 2 oraz art. 14 ust. 1, ust. 2 i ust. 3 RODO, a także sprawdzał, czy administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych objętych ochroną.

SIS II/VIS

Przedmiotem kontroli m.in. w Komendzie Głównej Policji było zbadanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. ustawą z 29 sierpnia 1997 r. o ochronie danych osobowych, ustawą o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679, Rozporządzeniem (WE) nr 1987/2006 oraz Decyzją Rady 2007/533/WSiSW.

System Informacyjny Schengen drugiej generacji (SIS II) jest systemem umożliwiającym krajowym sądom, prokuraturze, służbom policyjnym, granicznym, celnym oraz organom odpowiedzialnym za wykonanie przepisów dotyczących przemieszczania się obywateli państw trzecich i kontrolę w strefie Schengen oraz na jej granicach zewnętrznych, wymianę informacji dotyczących

m.in. osób poszukiwanych lub zaginionych, a także takich, którym odmówiono prawa do wjazdu i pobytu. W systemie są również rejestrowane dane dotyczące samochodów, broni palnej oraz dokumentów utraconych, skradzionych lub wykorzystanych do popełnienia przestępstwa. SIS ustanowiony został jako narzędzie rekompensujące zniesienie kontroli na granicach pomiędzy państwami obszaru Schengen. Jego istota polega na zapewnieniu, aby każde z państw będących stroną Konwencji Wykonawczej do Układu z Schengen posiadało ten sam zestaw informacji pozwalający na dostęp, przy pomocy zautomatyzowanych środków wyszukiwania, do wpisów dotyczących osób i przedmiotów w celu kontroli granicznej oraz innych kontroli policyjnych i celnych prowadzonych w ramach danego kraju oraz w celu wydawania wiz, dokumentów pobytowych i wykonywania przepisów prawnych o cudzoziemcach w kontekście stosowania wspomnianej konwencji.

Zakresem kontroli zostało objęte przetwarzanie przez Komendę Główną Policji danych osobowych w ramach Systemu Informacyjnego Schengen drugiej generacji (SIS II), w szczególności poprzez ustalenie:

- czy poza krajową kopią bazy danych SIS II („N.SIS II") funkcjonują inne kopie bazy danych SIS II, a jeżeli tak, to ile jest takich kopii i w jakich celach wykorzystywane są te kopie,
- w jaki sposób kopia/kopie bazy danych SIS II są aktualizowane,
- w jaki sposób rejestrowane są przypadki, w których uzyskano dostęp do danych SIS II lub dokonano wymiany tych danych,
- jakie informacje zawierają ww. rejestry,
- jak długo przechowywane są informacje w powyższych rejestrach,
- w jakich celach wykorzystywane są ww. rejestry,
- jak długo przechowywane są wpisy dotyczące osób wprowadzane do SIS II,
- w jaki sposób i kiedy weryfikowana jest potrzeba dokonania wpisu w SIS II,
- w jaki sposób i w jakim terminie od dokonania weryfikacji wpisy do SIS II są usuwane,
- w jaki sposób rejestrowana jest ocena stanowiąca podstawę do podjęcia decyzji o dłuższym przechowywaniu wpisu,
- w jaki sposób osoby, których dane dotyczą mogą realizować swoje prawo do dostępu do danych ich dotyczących przetwarzanych w SIS II,
- czy zostały opracowane i wdrożone procedury regulujące realizację ww. prawa,

czy zostały opracowane i wdrożone procedury związane z ryzykiem pomylenia osoby, której faktycznie dotyczy wpis, z osobą, której tożsamość jest przedmiotem pomyłki.

Po przeprowadzeniu kontroli i analizy całokształtu materiału zebranego w sprawie, pozyskanego w trakcie i po zakończeniu kontroli nie stwierdzono uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą w podmiocie kontrolowanym.

Kontrola została przeprowadzona także w Centralnym Organie Technicznym Krajowego Systemu Informatycznego (KSI), którym jest Komendant Główny Policji, w związku z dokonywanymi zmianami w KSI polegającymi na wdrożeniu nowej wersji interfejsu KSI SIS II (wersja: S.C. UI SIS 9.0.0) z 2 stycznia 2018 r., będącej wynikiem publikacji nowej wersji ICD dla CS.SIS (wersja 4.0.0) oraz rozszerzenia listy operacji o zapytania z wykorzystaniem obrazów linii papilarnych ExecuteFingerprintQuery oraz wynikających stąd nowych komunikatów KSINSExecuteFingerprintQuery oraz KSICSExecuteFingerprintQuery wraz z kodami błędów i ostrzeżeń. Stosownie bowiem do przepisów regulujących funkcjonowanie KSI, każda zmiana tego systemu wymaga uzyskania pozytywnej opinii organu nadzorczego.

Po przeprowadzeniu kontroli nie stwierdzono nieprawidłowości w KSI, który spełniał wymagania określone w art. 36–39 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych oraz w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych w zakresie objętym kontrolą. Wdrożenie nowej funkcjonalności w systemie centralnym

(C.SIS) umożliwiającej realizowanie zapytań biometrycznych z wykorzystaniem odcisków palców nie wpłynęło na architekturę systemu i było związane jedynie ze zwiększeniem funkcjonalności aplikacji. Nie stwierdzono konieczności modyfikacji infrastruktury, oprogramowania standardowego, infrastruktury kluczowej (PKI). Wobec tego została wydana pozytywna opinia w odniesieniu do funkcjonowania KSI po wprowadzonych zmianach.

Sądy

W 2018 r. odbyły się również cztery kontrole w sądach, których zakresem objęto sposób zabezpieczenia akt sądowych oraz przetwarzanie danych osobowych w związku z zastosowaniem systemów monitoringu wizyjnego na terenie obiektów sądowych. Jedna z ww. kontroli, została przeprowadzona w związku z doniesieniami medialnymi o odnalezieniu akt sądowych na terenie prywatnej posesji. W jej trakcie stwierdzono uchybienia w procesie przetwarzania danych osobowych, które zostały usunięte przez sąd bezpośrednio po zakończeniu czynności kontrolnych. W związku z powyższym nie było konieczności wszczęcia postępowania administracyjnego mającego na celu usunięcie nieprawidłowości.

5. Egzekucja administracyjna – zapewnienie wykonania decyzji

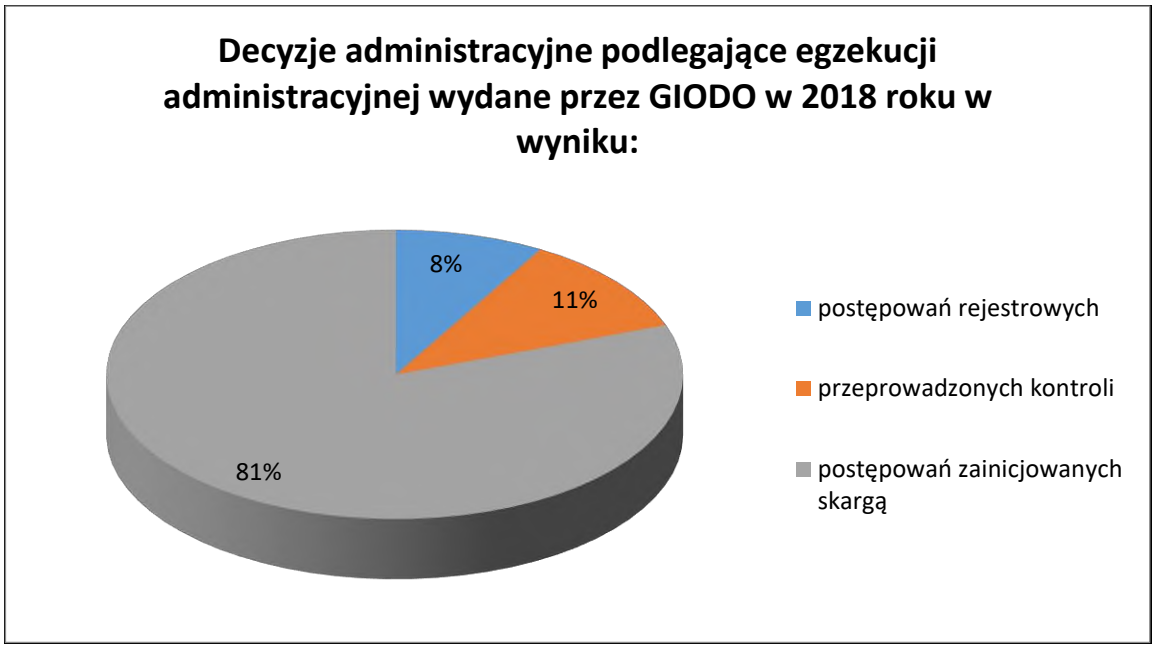
Działania egzekucyjne podjęte przez GIODO od 1 stycznia do 24 maja 2018 r.

W celu zapewnienia wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych, GIODO na podstawie art. 12 pkt 3 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych był uprawniony do stosowania środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji[146]. By to zadanie realizować GIODO został uznany za organ egzekucyjny w zakresie egzekucji administracyjnej obowiązków o charakterze niepieniężnym, a obowiązki z zakresu ochrony danych osobowych, nakładane w drodze decyzji GIODO znalazły się w katalogu obowiązków podlegających egzekucji administracyjnej.

Egzekucji administracyjnej podlegały wszystkie decyzje administracyjne GIODO nakładające na strony obowiązek (nakaz) do wykonania, które były ostateczne oraz te, którym nadano rygor natychmiastowej wykonalności. Jeżeli decyzja administracyjna zawiera postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlega egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek do wykonania nakładany na stronę (zobowiązanego) może polegać w szczególności 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 okresie od 1 stycznia do 24 maja 2018 r. **egzekucji administracyjnej podlegało 36 decyzji administracyjnych** GIODO zawierających nałożony na strony nakaz (obowiązek) do wykonania. Spośród decyzji wydanych w 2018 r. (do 24 maja) trzy dotyczyły postępowań rejestrowych, cztery decyzje zostały wydane w związku z przeprowadzonymi inspekcjami (kontrolami), **29** decyzji wydano na skutek postępowania zainicjowanego skargą. Największa liczba decyzji wydanych w związku z postępowaniem skargowym odzwierciedla liczbę skarg jakie wpłynęły do Biura GIODO, natomiast na najmniejszą liczbę decyzji wydanych w postępowaniach związanych z rejestracją zbiorów danych miał wpływ fakt, że obowiązek rejestracji zbiorów danych osobowych został zniesiony 25 maja 2018 r.

[146] Tj. Dz. U. z 2018 r. poz. 1314



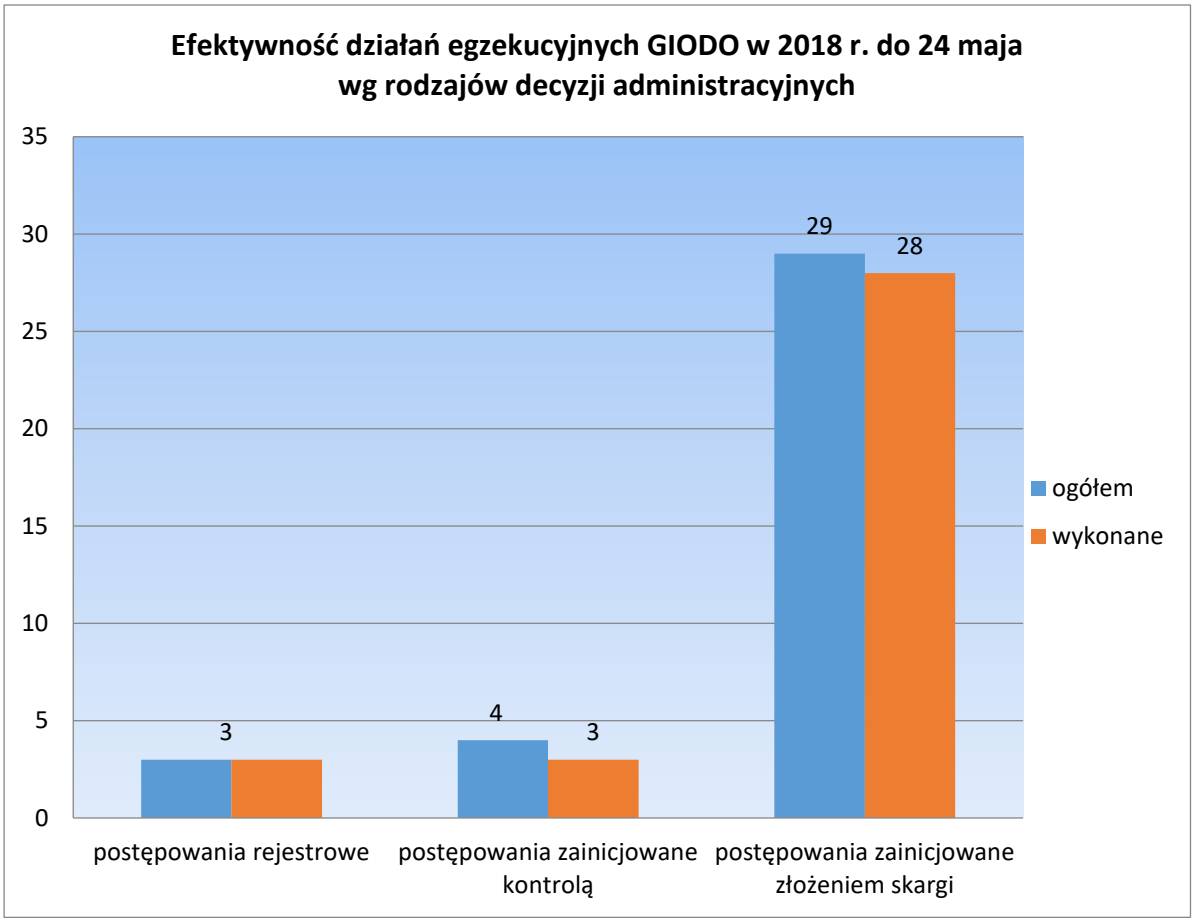
Wykres 1: **Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji wydanych przez GIODO do 24 maja 2018 r.**

Efektywność prowadzonych przez GIODO działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków w 2018 r. przedstawia się następująco: spośród 36 decyzji administracyjnych **wykonane zostały przez zobowiązanych 34 decyzje**, dwie decyzje na dzień 24 maja 2018 r. pozostały niewykonane.

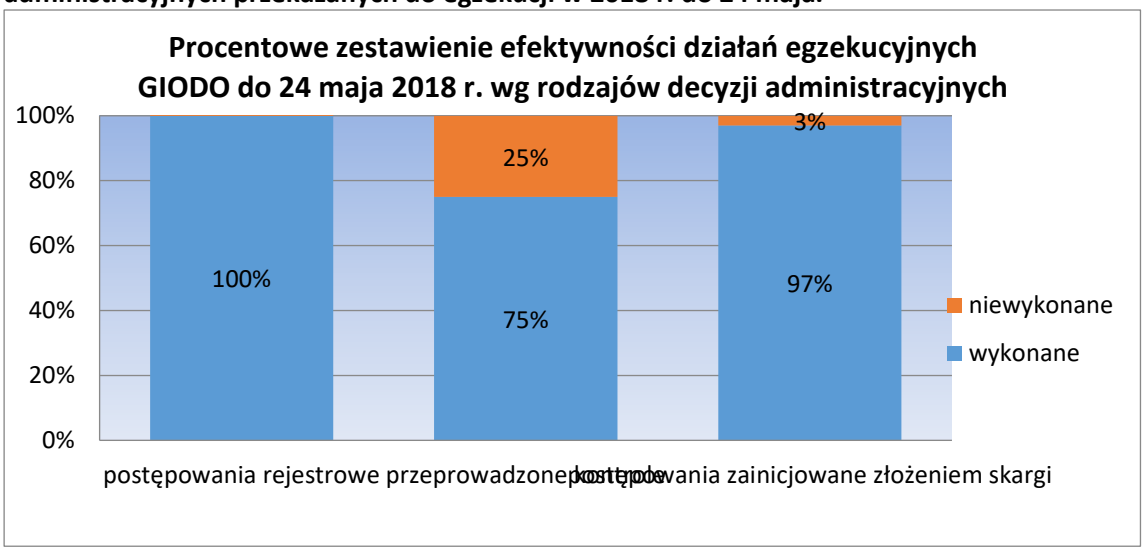
Decyzje te zostały objęte działaniami egzekucyjnymi już przez Prezesa UODO. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań Generalnego Inspektora. W 2 przypadkach wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia zobowiązany wykonał w całości decyzję administracyjną GIODO. Wobec drugiego zobowiązanego wystawiony został tytuł wykonawczy i wszczęte zostało postępowania egzekucyjne. Zastosowany został także środek egzekucyjny w postaci nałożenia grzywny w celu przymuszenia w wysokości 5 000 zł. Postępowanie egzekucyjne zostało zakończone w 2018 r. Zobowiązany wykonał decyzję Generalnego Inspektora, a nałożona grzywna na wniosek zobowiązanego została umorzona.

Spośród decyzji wydanych przez GIODO w 2018 r. i wykonanych przez zobowiązanych do 24 maja 2018 r. wskutek działań GIODO **trzy** dotyczyły postępowań rejestrowych, **trzy** zostały wydane w związku z przeprowadzonymi kontrolami, **28** wydano na skutek postępowania zainicjowanego skargą.

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych GIODO przekazanych do egzekucji do 24 maja 2018 r. wynosi **94 proc.** W odniesieniu do postępowań rejestrowych efektywność egzekucji wynosi **100 proc.**, wobec decyzji wydanych
w związku z przeprowadzonymi kontrolami wynosi **75 proc.**, natomiast w stosunku do decyzji wydanych na skutek postępowań zainicjowanych skargą wynosi **97 proc**.



Wykres 2: **Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu rodzajów decyzji administracyjnych przekazanych do egzekucji w 2018 r. do 24 maja.**

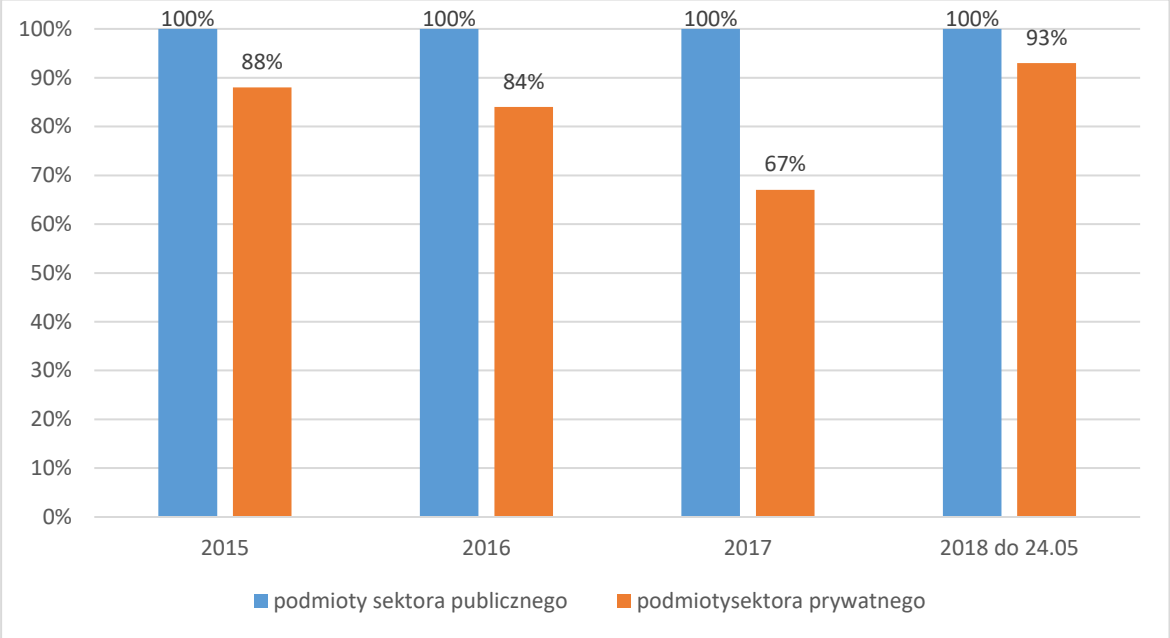


Wykres 3: **Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu rodzajów decyzji administracyjnych przekazanych do egzekucji w 2018 r. do 24 maja.**

Działania egzekucyjne do 24 maja 2018 r. dotyczyły decyzji skierowanych w 29 przypadkach do podmiotów z sektora prywatnego, a 7 przypadkach do sektora publicznego. Dwie niewykonane decyzje dotyczyły podmiotów z sektora prywatnego.

Analizując efektywność działań egzekucyjnych GIODO ze względu na przynależność zobowiązanych do sektora publicznego i sektora prywatnego (wykres nr 4), w latach 2015–2018 (do 24 maja), można zaobserwować w odniesieniu do podmiotów publicznych tendencję polegającą na stale utrzymującej się 100 proc. efektywności.

Natomiast procentowy wzrost efektywności działań skierowanych do zobowiązanych z sektora prywatnego w 2018 r. można wiązać ze wzrostem świadomości społecznej dotyczącej ochrony danych osobowych, który miał miejsce w związku ze zbliżającym się momentem rozpoczęcia stosowania RODO.



Wykres 4. **Zestawienie efektywności prowadzonych działań egzekucyjnych w odniesieniu do podmiotów z sektora publicznego i sektora prywatnego w latach 2015 – 2018 (do 24 maja).**

Działania egzekucyjne podjęte przez Prezesa UODO od 25 maja do 31 grudnia 2018 r.

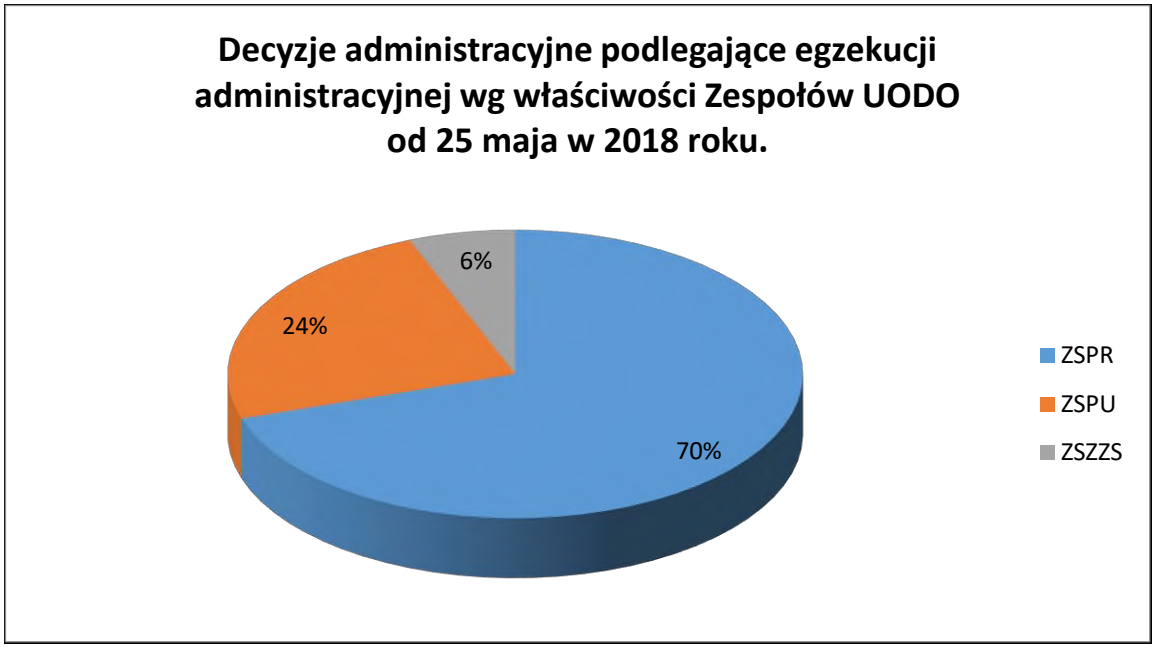
Z dniem 25 maja 2018 r. Generalny Inspektor Ochrony Danych Osobowych stał się Prezesem Urzędu Ochrony Danych Osobowych. Na podstawie art. 1a pkt 13 w zw. z art. 2 § 1 pkt 12 oraz art. 20 § 2 ustawy o postępowaniu egzekucyjnym w administracji Prezes UODO jest wierzycielem i organem egzekucyjnym w odniesieniu do egzekucji obowiązków o charakterze niepieniężnym z zakresu ochrony danych osobowych. W związku z tym, że Prezes UODO kontynuuje postępowania wszczęte przez GIODO przed 25 maja 2018 r. występuje również w roli wierzyciela i organu egzekucyjnego w odniesieniu do obowiązków o charakterze niepieniężnym nałożonych ostatecznymi decyzjami GIODO przed tą datą.

Ponadto, Prezes UODO jest również wierzycielem zakresie egzekucji należności pieniężnych (w szczególności administracyjnych kar pieniężnych, grzywien, kosztów upomnienia, kosztów egzekucyjnych, grzywien w celu przymuszenia, opłat za certyfikację oraz naliczonych od tych należności odsetek za zwłokę). Organem egzekucyjnym w zakresie egzekucji pieniężnych jest natomiast naczelnik właściwego urzędu skarbowego.

Należy zwrócić uwagę, że w celu zapewnienia wykonania obowiązków wynikających z decyzji administracyjnych, Prezes UODO – poza możliwością stosowania egzekucji administracyjnej – na podstawie art. 83 ust. 6 RODO zyskał nowe, istotne uprawnienie w postaci nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego na podstawie art. 58 ust. 2 RODO. Wysokość kary nałożonej w takim przypadku może sięgać 20 000 000 euro, a w przypadku przedsiębiorstwa w wysokości do 4 proc. jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Od 25 maja do 31 grudnia 2018 r. przeprowadzono dziewięć **kontroli** sprawdzających u zobowiązanych, z czego **osiem kontroli** potwierdziło wykonanie, bądź doprowadziło bezpośrednio do wykonania obowiązku wynikającego z decyzji.

Od 25 maja do 31 grudnia 2018 r. prowadzono **egzekucję administracyjną 50 decyzji administracyjnych** zawierających nałożony na strony nakaz (obowiązek) do wykonania o charakterze niepieniężnym. Dokonując podziału tych decyzji wg sektorów – **35** z nich dotyczyło właściwości sektora prywatnego, **12** – sektora publicznego oraz **trzy** z sektora zdrowia, zatrudnienia i szkolnictwa. W omawianym okresie UODO nie prowadziło działań egzekucyjnych wobec decyzji odnoszących się do sektora organów ścigania i sądów oraz z zakresu współpracy z administratorami danych.

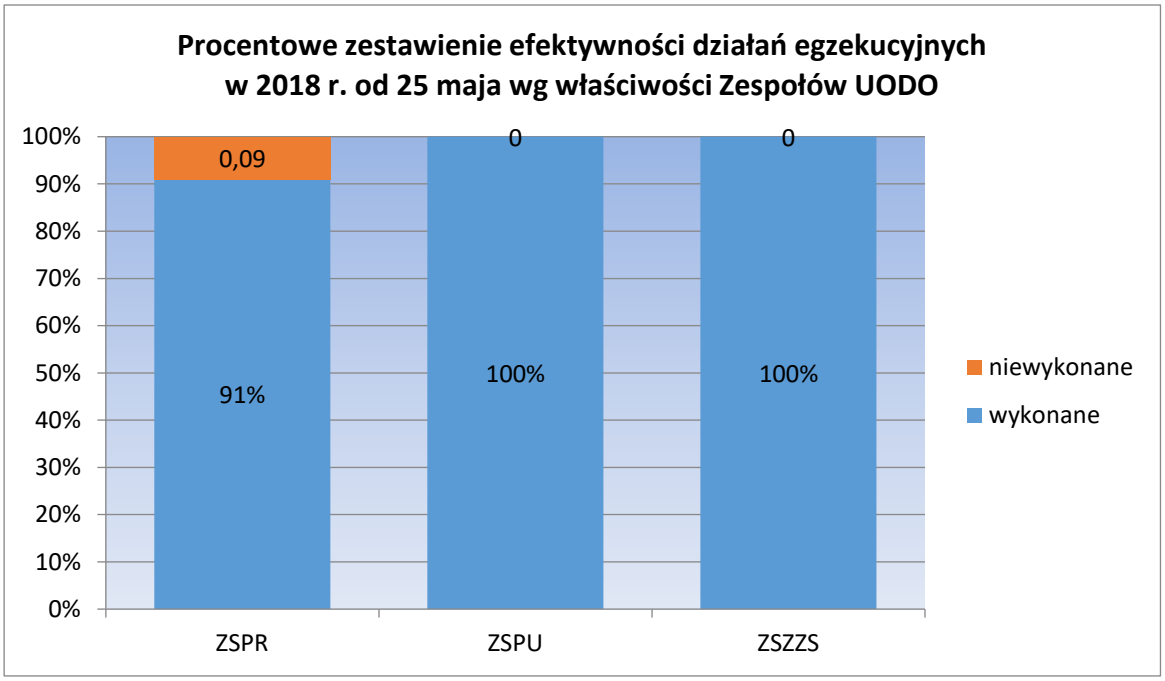


Wykres 5: **Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji wg właściwości Zespołów UODO, które je wydały.**

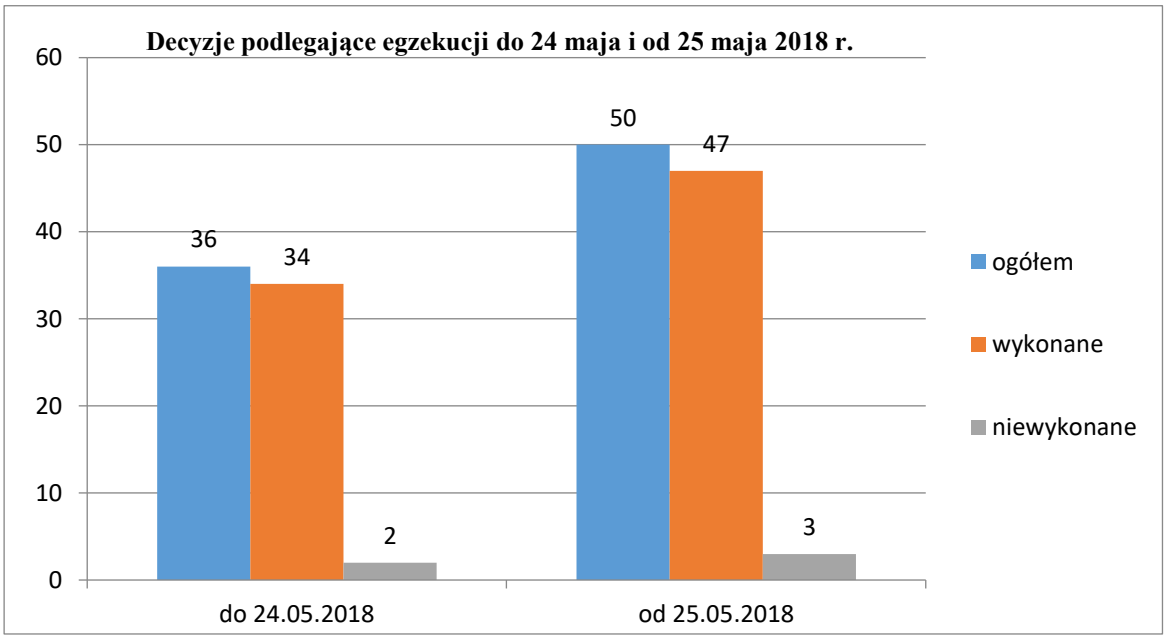
Efektywność prowadzonych działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków od 25 maja w 2018 r. przedstawia się następująco: spośród 50 decyzji **wykonanych zostało przez zobowiązanych 47 decyzji**, trzy decyzje do 31 grudnia 2018 r. pozostały niewykonane. Decyzje te zostały objęte działaniami egzekucyjnymi w 2019 r. Wykonanie decyzji nastąpiło wskutek pisemnych wezwań oraz kontroli przeprowadzonych u zobowiązanych UODO. W dwóch przypadkach wysłane zostało upomnienie w rozumieniu art. 15 ustawy o postępowaniu egzekucyjnym w administracji. Po otrzymaniu upomnienia w jednym przypadku zobowiązany wykonał w całości decyzję administracyjną. Wobec drugiego zobowiązanego działania egzekucyjne pozostały w toku w 2019 r.

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych przekazanych do egzekucji w 2018 r. po 24 maja wynosi **94 proc.**

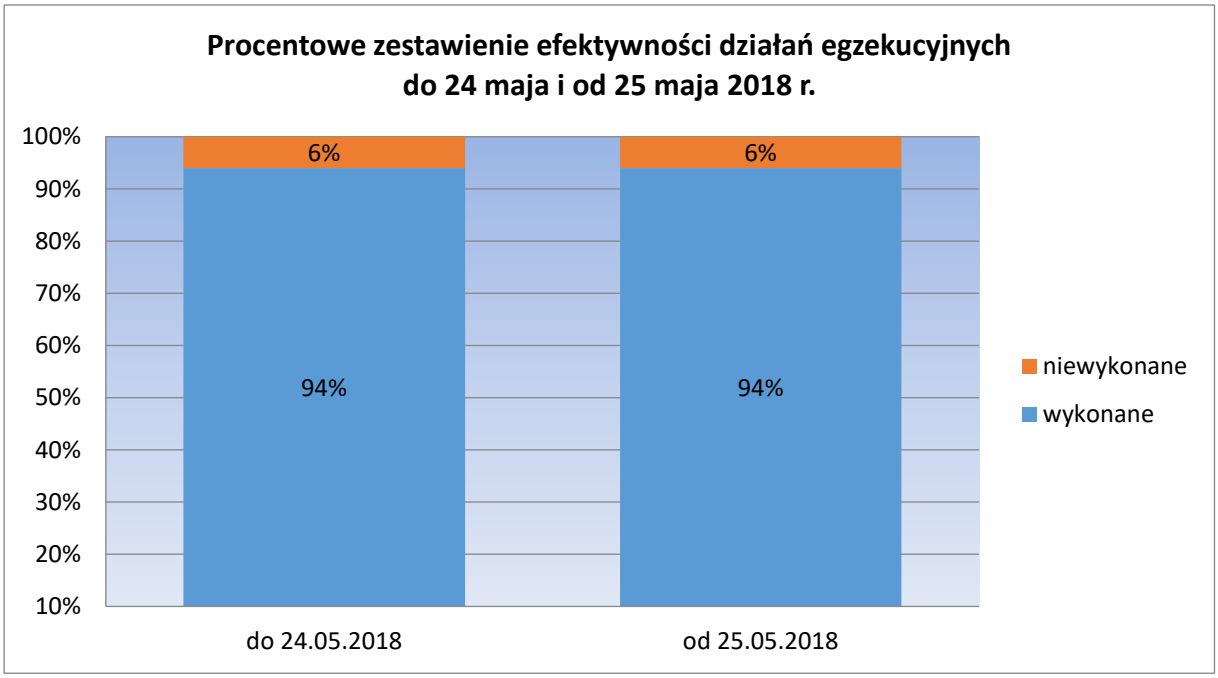
Wykres 6: **Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu rodzajów decyzji administracyjnych przekazanych do egzekucji w 2018 r.**



Wykres 7: **Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu do właściwości Zespołów UODO prowadzonych w 2018 r. od 25 maja.**



Wykres 8. **Zestawienie decyzji organu podlegających egzekucji administracyjnej i efektywność podejmowanych działań do 24 maja i od 25 maja 2018 r.**



Wykres 9. **Zestawienie procentowej efektywności działań egzekucyjnych organu do 24 maja i od 25 maja 2018 r.**

6. Opiniowanie projektów aktów prawnych i rozporządzeń dotyczących ochrony danych osobowych

Jednym z zadań organu nadzorczego jest opiniowanie projektów aktów prawnych, zarówno tych nowopowstających, jak i takich, które dotyczą tylko zmiany części przepisów prawa.
Rola organu w procesie legislacyjnym, na gruncie art. 12 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych sprowadzała się do opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych, natomiast stosownie do art. 51 ustawy z 10 maja 2018 r. o ochronie danych osobowych założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi UODO.

Zadanie to realizowane było w okresie sprawozdawczym poprzez analizy proponowanych zmian przepisów czy nowego brzmienia przepisów pod kątem ich zgodności do 24 maja 2018r. z ustawą z 29 sierpnia 1997 r. o ochronie danych osobowych, a później z przepisami rozporządzenia 2016/679. Propozycje te badane są pod względem m.in. stworzenia właściwych podstaw przetwarzania danych, zakresów danych podlegających przetwarzaniu, celów przetwarzania. Istotne jest przede wszystkim to czy projektodawca dokonał analizy wpływu przyjmowanych w przepisach rozwiązań na prywatność osób, których dane mają być przetwarzane. Ponadto analizowane są procesy, sposoby przetwarzania danych, udział podmiotów/organów w procesach przetwarzania danych, okresy retencji danych. Istotne jest także czy nowotworzone bądź zmieniane przepisy z danej dziedziny prawa/życia pozostają w zgodzie z zasadami przetwarzania danych wynikającymi z przepisów o ochronie danych osobowych.

Aktywny udział organu nadzorczego w procesie legislacyjnym ma na celu uczulenie projektodawców oraz ustawodawcy na stworzenie rozwiązań zgodnych z przepisami, nie tylko przyjaznych dla podmiotów stosujących prawo – administratorów czy podmiotów przetwarzających

zarówno z sektora publicznego, jak i prywatnego, ale także uwzględniających prawa osób, których dane osobowe są przetwarzane, na potrzeby publiczne czy prywatne.

Projektodawcy tworząc przepisy regulujące prowadzenie rejestrów zawierających dane osobowe albo uprawniające konkretne podmioty do przetwarzania danych często nie precyzują zakresów danych, jakie będą w tych rejestrach przetwarzane lub pozostawiają otwarty katalog takich danych. Kolejnym wskazywanym przez GIODO, a następnie Prezesa UODO, błędem jest brak określenia celu przetwarzania danych, który jest istotny tak do ustalenia zakresu ich pozyskania (adekwatności, proporcjonalności), jak i do zasad dalszego ich przetwarzania. Projektodawcy często używają sformułowania zgodnie z którym „celem przetwarzania danych jest realizacja zadań danego organu". Takie sformułowanie w przepisie jest zbyt szerokie i powoduje, że cel przetwarzania staje się niekonkretny. A to może rodzić obawę niezgodnego z prawem przetwarzania danych i niepewność co do ich bezpieczeństwa. Bardzo często mamy do czynienia z brakiem przepisów stanowiących o ograniczeniu czasowym przetwarzania danych osobowych (retencji danych). Jeżeli jednak taki okres zostaje wprowadzony w przepisie prawnym to zazwyczaj jest on zbyt długi w stosunku do celu przetwarzania danych.

Prezes UODO wielokrotnie postulował również odejście od koncepcji konkretnego wskazywania podmiotów, które mają pełnić rolę administratora danych. Przepisy RODO wskazują, że nie jest konieczne wyraźne wskazanie, sprecyzowanie administratora. Projektodawca powinien w przepisach wyznaczać, jakie cele będzie realizował podmiot przetwarzający dane i sposoby takiego przetwarzania, nie konkretyzując przy tym, kto ma być administratorem.

Błędem, na który Prezes UODO zwraca często uwagę jest też określanie przez projektodawcę w przepisach zgody jako podstawy prawnej do pozyskiwania i przetwarzania danych przez organy administracji państwowej. Jest to koncepcja nieprawidłowa z punktu widzenia konstytucyjnej zasady działania organów państwa na zasadzie i w granicach prawa. To znaczy, że przetwarzanie danych przez organy administracji państwowej ma mieć podstawę prawną w przepisie, a nie na podstawie udzielonej zgody, którą w każdej chwili można odwołać.

Częstym błędem popełnianym przez projektodawców jest również szczątkowe regulowanie przetwarzania danych osobowych, w tym danych szczególnie chronionych, w ustawach i dalsze doprecyzowywanie takiego przetwarzania w rozporządzeniach wykonawczych, będących przecież aktami prawnymi niższego rzędu w konstytucyjnym katalogu źródeł prawa lub regulowanie podstawy i procesów przetwarzania danych osobowych (również tych wrażliwych) wyłącznie w aktach podstawowych. Obowiązek regulowania takich kwestii w ustawie wynika wprost z art. 51 Konstytucji RP, statuującego tzw. zasadę autonomii informacyjnej jednostki.

Zapewnienie stosowania rozporządzenia 2016/679

Projekt **ustawy o zmianie niektórych ustaw w związku zapewnieniem stosowania rozporządzenia 2016/679**[147] (druk nr 3050). Do najistotniejszych kwestii zaliczyć można ograniczenia/wyłączenia w stosowaniu przepisów rozporządzenia 2016/679, uregulowanie monitoringu, określenie ról podmiotów w procesie przetwarzania danych osobowych czy podstaw prawnych przetwarzania danych osobowych.

W toku prac nad projektem Prezes UODO sygnalizował swoje zastrzeżenia do poszczególnych ustaw. Projekt przewidywał wiele wyłączeń i ograniczeń obowiązków wynikających z przepisów rozporządzenia 2016/679. W wielu ustawach, także m.in. w ustawie Ordynacja podatkowa, pojawiły się propozycje wprowadzenia przepisów zakładających profilowanie.

Uwagi Prezesa UODO częściowo zostały uwzględnione, jednakże w przyjętym ostatecznie kształcie projekt wciąż budzi wiele wątpliwości organu.

Prezes UODO zgłosił uwagi dotyczące następujących kwestii:

1) Zasada rozliczalności:

[147] ZSPU.023.109.2018

- **ustawa z dnia 21 marca 1985 r. o drogach publicznych** – organ nadzorczy zauważył, że regulacja wprowadzająca możliwość udostępnienia przez właściwy podmiot danych osobowych przetwarzanych w związku z poborem opłaty elektronicznej oraz przeciwdziałaniem niszczeniu dróg przez ich użytkowników za pomocą środków komunikacji elektronicznej i bez konieczności składania pisemnych wniosków nie zapewnia właściwemu podmiotowi należytej kontroli nad tym procesem;
- **ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych** – organ nadzorczy zauważył, że komentowana regulacja nie zapewnia ministrowi właściwemu do spraw informatyzacji kontroli nad tym procesem. Wydając decyzję administracyjną o zgodzie na udostępnienie danych z centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych, w trybie pełnej teletransmisji danych, minister właściwy do spraw informatyzacji może opierać się jedynie na oświadczeniu służb i organów wymienionych w art. 54a ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych, dodawanym przez art. 92 pkt 10 projektu.

2) Przetwarzanie szczególnych kategorii danych:

- **ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej** – Prezes UODO zakwestionował projektowaną dopuszczalność przetwarzania przez Komendanta Głównego Państwowej Straży Pożarnej, komendantów wojewódzkich Państwowej Straży Pożarnej, komendantów powiatowych (miejskich) Państwowej Straży Pożarnej, Rektora-Komendanta Szkoły Głównej Służby Pożarniczej, komendantów szkół Państwowej Straży Pożarnej, Dyrektora Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej i Dyrektora Centralnego Muzeum Pożarnictwa wszystkich szczególnych kategorii danych w odniesieniu do kandydatów na strażaków i strażaków Państwowej Straży Pożarnej;
- **ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej** – Prezes UODO podtrzymał swoje dotychczasowe stanowisko wobec upoważnienia służb statystyki publicznej do pozyskiwania danych genetycznych, wniósł o usunięcie z projektu uprawnienia służb statystyki publicznej do przetwarzania tak wysoce drażliwej kategorii danych, jakimi są dane genetyczne;
- **ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych** – projektowana regulacja przewidywała przedstawienie pracodawcy dokumentów potwierdzających dane osobowe o stanie zdrowia jako działanie dobrowolne. Prezes UODO zwrócił uwagę, że nie wiadomo, o jakich dokumentach jest mowa w przepisie, co może skutkować przekazywaniem pracodawcy różnych dokumentów, również nadmiarowych.

3) Zgoda na przetwarzanie danych osobowych:

- **ustawa z dnia 7 września 1991 r. o systemie oświaty** – projektowany przepis przewidywał pozyskiwanie zgody na przetwarzanie danych osobowych w celu zapewnienia bezpieczeństwa i ochrony zdrowia uczestnika. Prezes UODO wskazał, że w przypadku określonym w ustawie, podstawą prawną przetwarzania będzie art. 9 ust. 2 lit. g RODO, który stanowi, że przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym. W konsekwencji nadmiarowe i zbędne jest pozyskiwanie zgody na takie przetwarzanie danych od osoby, której przetwarzanie będzie dotyczyć.

4) Zasada minimalizacji danych:

- **ustawa z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej** – użyte w projekcie sformułowanie „w szczególności" daje możliwość przetwarzania danych przez administratora większej ilości danych i jako takie zostało przez organ nadzorczy oceniony negatywnie;
- **ustawa z dnia 23 maja 1991 r. o rozwiązywaniu sporów zbiorowych** – Prezes UODO zaproponował rezygnację ze sformułowania „co najmniej" – w dodawanym przez art. 19 projektu – art. 11 ust. 1^1 ustawy z dnia 23 maja 1991 r. o rozwiązywaniu sporów zbiorowych, gdyż wprowadzenie do komentowanego przepisu tego sformułowania skutkuje otwarciem katalogu danych osobowych, które mogłyby być przetwarzane w ramach jawnej listy mediatorów;

- **ustawa z dnia 13 października 1995 r. – Prawo łowieckie** – organ nadzorczy zwrócił uwagę, że celowym byłoby doprecyzowanie pojęcia „dane kontaktowe wnioskodawcy" poprzez wskazanie, jakie konkretnie dane wnioskodawcy wchodzą w zakres tego pojęcia. Niedookreślenie tego pojęcia może powodować, że zakres przetwarzanych danych osobowych będzie nadmierny w stosunku do celu, w którym są one przetwarzane;
- **ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych** – Prezes UODO osobowych zwrócił uwagę na użyte pojęcie „dane kontaktowe" (osoby ubiegającej się o wydanie legitymacji lub jej duplikatu), w związku z czym zaproponował jego dookreślenie;
- **ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych** Prezes UODO zaproponował rezygnację ze sformułowania „w szczególności" w dodawanym art. 58 ust. 1a ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, gdyż zamieszczenie tego sformułowania spowodowałoby możliwość pozyskiwania w ramach oświadczeń o stanie majątkowym dowolnej ilości danych;
- **ustawa z dnia 27 października 1994 r. o autostradach płatnych oraz**
- **Krajowym Funduszu Drogowym** – w swojej opinii Prezes UODO wnosił o uzupełnienie we wniosku podstawy prawnej żądania udostępnienia danych oraz określenia, czy udostępnienie takie ma charakter jednorazowy czy systematyczny. Dodatkowo Prezes UODO podkreślił, że w projekcie nie przewidziano gwarancji dla ochrony danych;
- **ustawa z dnia 21 listopada 2008 r. o służbie cywilnej** Prezes UODO zakwestionował art. 15 ust. 5 ustawy o służbie cywilnej, który przyznawałby Szefowi Służby Cywilnej uprawnienie do przetwarzania wszelkich danych osobowych członków korpusu służby cywilnej. W opinii Prezesa UODO przyznanie tak daleko idącego uprawnienia do przetwarzania danych osobowych Szefowi Służby Cywilnej mogłoby prowadzić do naruszenia praw członków korpusu służby cywilnej;
- **ustawa z dnia 17 lipca 2009 r. o systemie zarządzania emisjami gazów cieplarnianych i innych substancji** – zastrzeżenia Prezesa UODO budził szeroki zakres danych osobowych, które miałby by być przetwarzane w Krajowym systemie bilansowania i prognozowania emisji obejmujące równocześnie NIP i PESEL oraz adres e-mail, numer telefonu stacjonarnego i komórkowego (obligatoryjnie podawane). W opinii organu właściwego w sprawie ochrony danych osobowych podanie numeru telefonu i adresu poczty elektronicznej powinno być fakultatywne, a nie obligatoryjne;
- **ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie osób przebywających na obszarach wodnych oraz ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie i ratownictwie w górach i na zorganizowanych terenach narciarskich** – w przypadku obu ustaw – wprowadzono obowiązek sporządzenia wykazu odpowiednio – ratowników wodnych oraz ratowników górskich wraz z dokumentami potwierdzającymi spełnianie przez nich określonych warunków. Natomiast obowiązujące przepisy przewidują jedynie pozyskiwanie informacji o liczbie ratowników wodnych i górskich oraz posiadanych przez nich kwalifikacjach przydatnych w danym rodzaju ratownictwa, nie jest jasny cel, dla którego w projekcie zdecydowano się na pozyskiwanie zindywidualizowanych danych ratowników wodnych i górskich.

5) Retencja danych:

- **ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej** – Prezes UODO sprzeciwił się okresowi przechowywania danych w Operacie do badań statystycznych – 100 lat;
- **ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym** – wątpliwości organu właściwego w sprawie ochrony danych osobowych budził długi okres przetwarzania przez KNF szczególnych kategorii danych osobowych (25 lat);
- **ustawa z dnia 14 grudnia 2012 r. o odpadach** – zgodnie z propozycją „dane osobowe […] przechowuje się […] bezterminowo – w przypadku pozostałych danych". Takie brzmienie zostało

zanegowane przez organ nadzorczy, pozostawało bowiem w oczywistej sprzeczności z zasadą ograniczenia przechowywania, o której mowa w art. 5 ust. 1 lit. e RODO.

6) Obowiązek informacyjny:

- **ustawa z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych**; **ustawa z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych**; **ustawa z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych**; **ustawa z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym**; **ustawa z dnia 8 grudnia 2017 r. o Sądzie Najwyższym**– odnosząc się do kwestii obowiązku informacyjnego, organ nadzorczy wskazał, że prawodawca unijny jako zasadę przyjął indywidualne powiadamianie osoby, której dane dotyczą uzasadnienia nie znajduje zatem – w ocenie Prezesa UODO – realizowanie obowiązku informacyjnego z art. 13 rozporządzenia 2016/679 wyłącznie przez umieszczenie informacji na stronie podmiotowej Biuletynu Informacji Publicznej oraz w widocznym miejscu w budynku Trybunału Konstytucyjnego, sądu.

7) Zautomatyzowane przetwarzanie, profilowanie:

- **ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa** – ustawodawca przewidział zautomatyzowane przetwarzanie, w tym profilowanie, które mogłoby opierać się także na danych osobowych ujawniających pochodzenie rasowe lub etniczne oraz danych biometrycznych. Prezes UODO podkreślił niezgodność w tym zakresie z przepisami RODO;
- **ustawa z dnia 6 września 2001 r. o transporcie drogowym** – Prezes UODO zwrócił uwagę na przepis wprowadzający uprawnienie dla Inspekcji Transportu Drogowego do profilowania w związku z realizacją przez ten podmiot zadań, o których mowa w ustawie. Organ nadzorczy stwierdził, że przyjęcie takiego rozwiązania jest niewystarczające i naraża projektodawcę na odpowiedzialność za uchwalenie przepisów prawa niezgodnych z elementarnymi zasadami rozporządzenia 2016/679, jak również godzi w podstawowe prawa i wolności osób, których dane osobowe miałyby być w taki sposób przetwarzane;
- **ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych** – Prezes UODO wskazał na uprawnienie przyznane dla Ubezpieczeniowego Funduszu Gwarancyjnego do podejmowania decyzji w indywidualnych przypadkach w oparciu o zautomatyzowane przetwarzanie danych, w tym profilowanie, uznając przesłankę do profilowania za niewystarczającą. Podkreślił, że artykuł 22 ust. 2 lit. b rozporządzenia 2016/679 wskazuje wyraźnie, że zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie, jest dopuszczalne wyłącznie w oparciu o przepisy szczegółowo regulujące zasady zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania, przewidujące przy tym właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Ponadto Prezes UODO zgłaszał uwagi do następujących ustaw zmienianych w omawianym projekcie:

Zmiany w ustawie Prawo bankowe

wyjaśnianie podstaw podjętych decyzji kredytowych zagwarantowane także osobom fizycznym – propozycja rozszerzenia prawa do wyjaśniania podstaw podjętej decyzji na wszystkie decyzje kredytowe (także te podejmowane z udziałem człowieka). Przekazywane informacje powinny następować nie tylko poprzez bardzo ogólne „wyjaśnienie" podstaw podjętej przez bank decyzji, ale – w odpowiednim przepisie aktualnie zmienianego Prawa bankowego – wskazane powinno być wprost i jednoznacznie, że osobie, której dane dotyczą, przekazywane są (będące elementem obowiązku informacyjnego) informacje, o których mowa w przepisach rozporządzenia 2016/679, o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, a mianowicie „istotne informacje o zasadach ich podejmowania, o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania

dla osoby, której dane dotyczą Prezes UODO popierał propozycję rozszerzenia prawa do wyjaśnienia podstaw podjętej decyzji na wszystkie decyzje kredytowe;

- sprzeciw wobec propozycji Związku Banków Polskich dotyczącej otwarcia katalogu danych podlegających profilowaniu;
- podejmowanie zautomatyzowanych decyzji, w tym profilowanie w celu oceny zdolności kredytowej i analizy ryzyka kredytowego przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów, instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, a także instytucje utworzone na podstawie art. 105 ust. 4 mogą – pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, zakwestionowania tej decyzji, wyrażenia własnego stanowiska oraz do uzyskania interwencji ludzkiej oraz wyłącznie w oparciu o kategorie danych enumeratywnie wymienione w przepisie zawierającym zamknięty katalog danych, które mogą być wykorzystywane przez banki w procesie profilowania;
- postulaty dotyczące „otwarcia" katalogu danych mających być wykorzystywanymi w procesie profilowania nie zostały poparte szczegółowym ich uzasadnieniem – nie została wykazana przez projektodawcę niezbędność przyjęcia rozwiązania polegającego na niczym nieskrępowanym przetwarzaniu przez banki wszelkich możliwych danych osobowych dla dokonania oceny zdolności kredytowej, w tym szczególnych kategorii danych – wprowadzenie otwartego katalogu danych poprzez dodanie kategorii „inne dane niezbędne z uwagi na właściwą ocenę celu kredytu", jest wysoce niebezpieczne z punktu widzenia ochrony danych osobowych, właśnie ze względu na nieokreśloność zakresu danych mających być wykorzystywanymi w procesie profilowania oraz bardzo szerokie możliwości doboru kategorii danych – sprzeczność z art. 32 Konstytucji RP konstytucyjnym zakazem dyskryminacji obywateli oraz z przepisami o ochronie danych osobowych, w tym m.in. z motywem 54 rozporządzenia 2016/679[148], a przyjęcie zaproponowanego rozwiązania stwarza poważne ryzyko pozyskiwania i dalszego przetwarzania przez banki i inne instytucje wskazane w art. 105a ust. 1a Prawa bankowego szczególnych kategorii danych[149] oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa[150].Prezes UODO wskazał, że proponowane rozwiązanie polegające na profilowaniu warunkującym zawarcie umowy stoi w sprzeczności motywem 93 rozporządzenia 2016/679 nakładającym obowiązek przeprowadzenia oceny skutków dla ochrony danych osobowych. Prezes UODO postulował o pozostawienie zamkniętego katalogu danych osobowych, które mają być przetwarzane w związku z art. 105a ust. 1a Prawa bankowego.

W wyniku prac nad zmianą ustawy katalog danych został doprecyzowany, ale nie został zamknięty, niemniej przyjęto, że zautomatyzowane decyzje mogą być podejmowane wyłącznie w oparciu o dane niezbędne z uwagi na cel i rodzaj kredytu oraz że nie mogą być podejmowane w oparciu o dane, o których mowa w art. 9 rozporządzenia 2016/679.

Zmiany w ustawie o działalności ubezpieczeniowej i reasekuracyjnej[151]:

- konieczność zapewnienia spójności tej ustawy z przepisami ustawy o Prawach pacjenta i Rzeczniku Praw Pacjenta. Ustawa o Prawach pacjenta (…) przewidywała bowiem możliwość

[148] Przetwarzanie danych dotyczących zdrowia z uwagi na względy interesu publicznego nie powinno skutkować przetwarzaniem danych osobowych do innych celów przez strony trzecie, takie jak pracodawcy, czy zakłady ubezpieczeń i banki.

[149] Danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych dotyczących zdrowia, danych biometryczne, danych genetycznych, danych o seksualności lub orientacji seksualnej (art. 9 ust. 1 rozporządzenia 2016/679).

[150] Art. 10 rozporządzenia 2016/679.

[151] Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2019 r. poz. 381).

udostępnia szeroko rozumianej dokumentacji medycznej zakładom ubezpieczeń, za zgodą pacjenta, natomiast organ nadzorczy wskazywał, że przepisy ustawy o Prawach pacjenta i Rzeczniku Praw Pacjenta nie powinny dawać szerszego dostępu zakładom ubezpieczeń do dokumentacji medycznej niż przepisy ustawy o działalności ubezpieczeniowej i reasekuracyjnej. Konieczność przyjęcia rozwiązań dających większe gwarancje ochrony danych osobowych, praw i wolności – dostęp do dokumentacji medycznej powinien być ograniczony tylko do informacji o aktualnym stanie zdrowia, powinien dotyczyć tylko historii choroby określającej aktualny stan zdrowia, konieczne są w przepisach gwarancje, że informacja będzie następować z wyłączeniem: informacji o rokowaniach, wyników badań genetycznych/ danych genetycznych, danych biometrycznych, danych osób trzecich, z zachowaniem rozwiązania polegającego na oznaczaniu kodem jednostki chorobowej;

- powinien być też określony cel i niezbędność przetwarzania danych osobowych poprzez wskazanie rodzajów umów, dla których poszczególne informacje byłyby konieczne, np. umowa ubezpieczenia na życie, kryteria, kiedy informacje o stanie zdrowia są niezbędne zakładowi ubezpieczeń dla zawarcia, zmiany oraz wykonania umowy ubezpieczenia oraz w celu oceny roszczeń.

Ostatecznie znowelizowane przepisy ustawy o działalności ubezpieczeniowej i reasekuracyjnej zezwalają, podobnie jak w Prawie bankowym, na przetwarzanie danych z art. 9 rozporządzenia 2016/679 dotyczące zdrowia ubezpieczonych lub uprawnionych z umowy ubezpieczenia, zawarte w umowach ubezpieczenia lub oświadczeniach składanych przed zawarciem umowy, w celu oceny ryzyka ubezpieczeniowego lub wykonania umowy ubezpieczenia, w zakresie niezbędnym z uwagi na cel i rodzaj ubezpieczenia. Katalog danych w oparciu o które mogą być podejmowane zautomatyzowane decyzje został zamknięty. Spośród informacji jakie mogą być zasięgane przez zakład ubezpieczeń, dotyczących historii choroby pacjenta wyeliminowano możliwość pozyskiwania od lekarza czy placówki zdrowotnej informacji o „rokowaniach". Dane z art. 10 rozporządzenia 2016/679 są przetwarzane w przypadku określonym w art. 42 ust. 2a ustawy.

Zmiany w ustawie o świadczeniu usług drogą elektroniczną[152]

- katalog danych osobowych usługobiorcy, które usługodawca może przetwarzać w celu nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego[153] – organ nadzorczy wskazał, że stosowanie jak i kontrola tych przepisów podlegać powinny i będą zasadom przetwarzania danych osobowych wynikającym z art. 5 rozporządzenia 2016/679, i dlatego pozostawienie przedmiotowego katalogu danych można uznać za właściwe;
- wątpliwości budził ust. 4 art. 18 wprowadzony na etapie prac komisji sejmowych – Komisji Administracji i Spraw Wewnętrznych oraz Komisji Sprawiedliwości i Praw Człowieka, gdyż wprawdzie nie wprost, niemniej jednak, wydaje się on tworzyć podstawę prawną do przetwarzania przez usługodawcę danych osobowych usługobiorcy celem podejmowania zautomatyzowanych decyzji w tym profilowania usługobiorców. Zmiana ta wskazuje, że przetwarzanie danych dla takich celów ma się odbywać za zgodą usługobiorcy i ma się opierać na „innych danych dotyczących usługobiorcy, które nie są niezbędne do świadczenia usługi droga elektroniczną" – oznacza to, że zarówno dane osobowe, o których mowa w ust. 1 art. 18 ustawy o świadczeniu usług drogą elektroniczną, jak i inne dane, a zatem także te należące do szczególnych kategorii danych, a zebrane przez usługodawcę w trakcie świadczenia usługi drogą elektroniczną, mogą być wykorzystywane do profilowania usługobiorców;
- o ile tego rodzaju przetwarzanie danych miałoby się opierać na zgodzie osoby, której dane dotyczą[154], to zgoda taka musi być wyraźna;

[152] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2019 r. poz. 123) – dalej: ustawa o świadczeniu usług drogą elektroniczną.

[153] Art. 18 ust. 1 i ust. 2 ustawy o świadczeniu usług drogą elektroniczną.

[154] Co jest dopuszczalne mocą art. 22 ust. 2 lit c) rozporządzenia 2016/679

- ze względu na art. 22 ust.3 rozporządzenia 2016/679[155], w przypadku, gdy zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie miałoby się opierać na zgodzie, której dane dotyczą, to nie dość, że zgoda ta powinna być wyraźna, to jeszcze administrator obowiązany jest wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
- we wprowadzanych przepisach brak jest gwarancji, że usługodawcy profilujący usługobiorców nie mogą opierać się na ich szczególnych kategoriach danych osobowych. Do przetwarzania takich danych może dochodzić, skoro przepisy mogą dotyczyć wszelkich usług świadczonych drogą elektroniczną, w tym serwisów, w których mogą przetwarzane mogą być dane należące do szczególnych kategorii, takie jak np. dane dotyczące zdrowia, ujawniające poglądy polityczne, przekonana religijne i światopoglądowe, dane o seksualności.

Inne projekty aktów prawnych przesłanych do zaopiniowania przez GIODO lub Prezesa UODO:
Powszechny spis rolny i narodowy spis powszechny ludności i mieszkań
Prezes UODO otrzymał do zaopiniowania projekt **ustawy o powszechnym spisie rolnym w 2020 r.**[156] oraz projekt **ustawy o narodowym spisie powszechnym ludności i mieszkań w 2021 r.**[157] W uwagach do obu projektów organ nadzorczy wyraził swój sprzeciw w stosunku do okresu retencji, który przewidywany jest na sto lat. Projektodawca nie wskazał w uzasadnieniach istotnych powodów, które przemawiałyby za takim wydłużeniem okresu przechowywania przez służby statystyki publicznej danych osobowych, które mają być zebrane w powszechnym spisie rolnym w 2020 r. i narodowym spisie powszechnym ludności i mieszkań w 2021 r. (dotychczas dane takie były przechowywane przez okres dwóch lat od dnia zakończenia spisu).

2)Koncepcja nowego Prawa Zamówień Publicznych
Prezes UODO uwzględniając szybki postęp technologiczny i globalizację, które przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych, opiniował materiał przygotowany przez Ministerstwo Przedsiębiorczości i Technologii wspólnie z Urzędem Zamówień Publicznych pn. „Koncepcja nowego Prawa Zamówień Publicznych”[158]. Organ nadzorczy, analizując proponowane rozwiązanie, zwraca szczególną uwagę, że dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. W uwagach do projektu Prezes UODO podkreślił, że dane osobowe powinny być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, a więc przepisy jednoznacznie powinny wskazywać ostateczny termin, po upływie którego dane powinny być usunięte lub zanonimizowane.

Podkreślono również, że każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania (*privacy by design*), a także powinna być zakładana domyślna ochrona danych w systemie (*privacy by default*). Rozważania organu skierowane zostały również na gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

W opinii Prezesa UODO zachodzi również konieczność dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dokonanie takiej oceny przez administratora jest konieczne przed rozpoczęciem przetwarzania, jeżeli taki rodzaj przetwarzania –

[155] Zgodnie z art. 22 ust. 3 rozporządzenia 2016/679 administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia stanowiska i do zakwestionowania tej decyzji.
[156] ZSPU.023.82.2018
[157] ZSPU.023.54.2018
[158] ZSPU.023.16.2018

w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Zintegrowana Platforma Analityczna

Kolejnym opiniowanym przez Prezesa UODO aktem był projekt dokumentu pn. Opis założeń projektu informatycznego **„Zintegrowana Platforma Analityczna"**. Celem projektu – co wynikało już z jego wstępnej analizy – było utworzenie systemu teleinformatycznego o nazwie „Zintegrowana Platforma Analityczna", do którego miałyby być przekazywane dane z licznych rejestrów i baz danych. Zaproponowane przez projektodawcę rozwiązania budziły istotne wątpliwości Prezesa UODO, które zostały wyrażone pismem z sierpnia 2018 r. Organ nadzorczy przypomniał, że prawodawca unijny w motywie 31 do rozporządzenia 2016/679 zasugerował zachowanie daleko idącej ostrożności w kwestii przyznawania organom publicznym uprawienia do pozyskiwania danych osobowych. Prezes UODO wyraził wątpliwość co do celu utworzenia Zintegrowanej Platformy Analitycznej, pod kątem możliwości dublowania przez Ministra Cyfryzacji w praktyce prac wykonywanych przez powołany do tego typu zadań podmiot – Główny Urząd Statystyczny.

Ustawa o uchyleniu ustawy o strażach gminnych oraz o zmianie innych ustaw[159]

Prezes Urzędu Ochrony Danych Osobowych wskazał, że projekt z uwagi na swój charakter oraz zakres stwarza duże prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Straże gminne podczas swojej działalności zgromadziły znaczną ilość danych wśród których mogą znajdować się dane osobowe różnego rodzaju. W projekcie nie określono postępowania z dotychczas posiadanymi danymi osobowymi – czy mają zostać przekazane, a jeśli tak, to do czego mają służyć, czy też mają zostać usunięte. Ponadto nie wskazano żadnej formy retencji danych osobowych, ani okresu tej retencji.

Dodatkowo Prezes UODO zgłosił uwagi szczegółowe do art. 2, który przewidywał powołanie komisji weryfikacyjnych, których zadaniem jest przeprowadzenie postępowania weryfikacyjnego strażników gminnych zatrudnionych w strażach gminnych działających na terenie danego województwa. Wątpliwości wzbudził brak określenia przepisów w zakresie wskazania danych osobowych, jakie komisja weryfikacyjna może przetwarzać w ramach postępowania weryfikacyjnego. Wskazanie tych danych jest o tyle istotne, że komisja weryfikacyjna może w ramach postępowania weryfikacyjnego przetwarzać również szczególne kategorie danych osobowych w rozumieniu art. 9 i 10 RODO m.in. dotyczące stanu zdrowia kandydatów. Brak precyzyjnego określenia danych narusza zasadę przejrzystości (wyrażoną w art. 5 ust. 1 lit. a RODO) oraz zasadę minimalizacji danych (wskazaną w art. 5 ust. 1 lit. c RODO).

Wspieranie rodziny i system pieczy zastępczej

Prezes UODO brał udział w opiniowaniu projektu **ustawy o zmianie ustawy o wspieraniu rodziny i systemie pieczy zastępczej oraz niektórych innych ustaw[160]**. Szczególnie istotne zagrożenia z punktu widzenia ochrony danych osobowych, które były wskazywane przez PUODO dotyczyły znajdujących się w projekcie przepisów tworzących wykazy prowadzone przy użyciu systemu teleinformatycznego zapewnianego przez ministra właściwego do spraw rodziny. Organ nadzorczy wskazywał m.in. na brak przeprowadzenia przez projektodawcę oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych w rozumieniu art. 35 ust. RODO w związku z tworzeniem wykazów oraz na brak wskazania trybu udostępniania danych osobowych z wykazów.

[159] ZSPU.023.94.2018
[160] ZSPU.023.130.2018

Ponadto w projekcie w sposób ogólnikowy sformułowano cel udostępniania z wykazów przetwarzanych danych osobowych, nie określono trybu, w jakim dane miały być udostępniane. Prezes UODO wskazał, że ze względu na szeroki katalog danych osobowych, szczególne kategorie danych, dostęp do danych zawartych w wykazach powinien odbywać w trybie wnioskowym i w ściśle skonkretyzowanym celu. Dostęp do tych danych powinien być dokładnie regulowany i poddawany ścisłej okresowej kontroli, tak aby możliwe było przeciwdziałanie możliwym nadużyciom polegającym na nieuzasadnionym pozyskiwaniu danych, zwłaszcza jeżeli dostęp ten miałby odbywać się drogą elektroniczną.

Realizowanie usług społecznych przez centrum usług społecznych

Prezes UODO brał udział w opiniowaniu **projektu ustawy o realizowaniu usług społecznych przez centrum usług społecznych**[161], gdzie kwestionował wiele rozwiązań naruszających przepisy RODO. Projekt ustawy przewidywał, że rada gminy może przyjąć w drodze uchwały program usług społecznych, w którym zawarto unormowania powalające na zawarcie w programie usług społecznych danych należących do szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 i 10 RODO. W art. 5 ust. 5 wskazano, że program usług społecznych jest udostępniany na stronie Biuletynu Informacji Publicznej urzędu gminy oraz na stronie Biuletynu Informacji Publicznej centrum, a co za tym idzie upublicznianie danych, należących od szczególnych kategorii danych osobowych. Prezes UODO zwrócił uwagę, że wskazany w art. 2 projektu zakres usług społecznych oraz ustaw, na podstawie których te usługi będą świadczone, jest bardzo szeroki i istotnie w wielu przypadkach do ich realizacji potrzebne może być przetwarzanie danych osobowych różnego typu ze szczególnych kategorii, o których mowa w art 9 ust. 1 i art. 10 RODO. Organ nadzorczy nie kwestionuje co do zasady możliwości zawarcia w projekcie przepisów dających podstawę do przetwarzania ww. kategorii danych osobowych, jednakże tylko przy uwzględnieniu warunków wskazanych w art. 9 ust. 2 i art. 10 RODO.

Krajowa Administracja Skarbowa

Prezes UODO w opinii do projektu **ustawy o zmianie ustawy o Krajowej Administracji Skarbowej oraz niektórych innych ustaw**[162] kwestionował wiele rozwiązań naruszających przepisy RODO. Szczególnie istotne zagrożenia z punktu widzenia ochrony danych osobowych, które były kwestionowane w projekcie przez Prezesa UODO dotyczyły funkcjonowania Centralnego Rejestru Danych Podatkowych, która to baza ma służyć do przetwarzania danych pozyskanych z baz, rejestrów, ewidencji, zbiorów i systemów informatycznych udostępnionych organom KAS w celu realizacji ustawowych zadań. Zawarte w projekcie przepisy dotyczące Centralnego Rejestru Danych Podatkowych w opinii organu nadzorczego naruszały zasadę zgodności z prawem, rzetelności i przejrzystości wyrażoną w art. 5 ust. 1 lit. a RODO oraz zasadę ograniczonego celu wskazaną w art. 5 ust. 1 lit b. Projektodawca nie doprecyzował, jakie dane mogą być pozyskane i z jakich baz danych oraz nie wskazano precyzyjnie celu przetwarzania danych.

Ordynacja podatkowa

Prezes UODO brał udział w opiniowaniu projektu **ustawy – Ordynacja podatkowa**[163]. Organ nadzorczy wskazał, że projekt – z uwagi na swój charakter oraz zakres – stwarza duże prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Szczególnie istotne zagrożenia z punktu widzenia ochrony danych osobowych, które były wskazywane w projekcie przez Prezesa UODO dotyczyły nadania uprawnień dla Krajowej Informacji Skarbowej do przetwarzania danych biometrycznych w rozumieniu art. 4 pkt 14 RODO przetwarzanych w trakcie udzielenia

[161] ZSPU.023.205.2018

[162] ZSPU.023.91.2018, (Dz. U. z 2018 r. poz. 2354)

[163] ZSPU.023.53.2018

informacji telefonicznej przez pracowników tego organu w celu zidentyfikowania lub weryfikacji tożsamości osoby fizycznej. Zawarty w projekcie przepis dotyczący przetwarzania ww. danych biometrycznych w opinii organu nadzorczego naruszał art. 5 ust. 1 lit. a RODO w zakresie jakim nie precyzował danych, jakie mają być przetwarzane oraz art. 9 ust. 1 RODO, w związku z art. 9 ust. 2 lit. g RODO, w zakresie w jakim projektowany przepis nie zapewnia wymogu proporcjonalności. Ponadto nie przeprowadzono oceny skutków uzasadniającej taką ingerencję w prawo do prywatności osób, w sytuacji gdy wobec nich nie są przeprowadzone jakiekolwiek postępowania. W ocenie organu nadzorczego może to rodzić także zarzut naruszenia konstytucyjnych uprawnień jednostki, która ma prawo oczekiwać pozyskiwanie takich danych w szczególnych sytuacjach wraz z całą procedurą określającą, jaki jest dalszy proces ich przetwarzania (cele, retencja, podmioty korzystające z tych danych).

Ponadto organ nadzorczy wskazał na potrzebę precyzyjnego określenia okresu retencji danych osobowych w celu przeciwdziałania wykorzystywania sektora finansowego do wyłudzeń skarbowych np. danych pozyskanych na skutek profilowania. Brak regulacji w tym zakresie (kryteriów kształtujących terminy usuwania danych nadmiarowych, zbędnych) powoduje naruszenie zasad wyrażonych w art. 5 ust. 1 RODO. Dane osobowe powinny być przechowywane przez okres nie dłuższy niż jest to konieczne do celów, w których dane te są niezbędne.

Uwagi organu do spraw ochrony danych osobowych zostały częściowo uwzględnione, odstąpiono od rozwiązania pozwalającego na przetwarzanie danych biometrycznych.

Oferta publiczna

Przedmiotem opiniowania był projekt **ustawy o zmianie ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz niektórych innych ustaw**[164]. Prezes UODO z punktu widzenia przepisów RODO – zgłosił uwagi dotyczące zarówno przepisów normujących zasady upubliczniania na stronie internetowej Komisji Nadzoru Finansowego, informacji związanych z nakładaniem kar pieniężnych, możliwości wykluczenia papierów wartościowych z obrotu oraz nakazu zaprzestania działań skutkujących powstaniem naruszeń, jak i niedoprecyzowania w składanych do Komisji Nadzoru Finansowego wnioskach z danymi kontaktowymi emitenta lub oferującego lub ustanowionego w sprawie pełnomocnika emitenta lub oferującego katalogu tych danych w szczególności:

- uwaga do art. 1 pkt 29 lit. a projektu **– została uwzględniona** poprzez zamknięcie katalogu danych kontaktowych we wnioskach składanych przez emitenta lub oferującego lub ustanowionego w sprawie pełnomocnika emitenta lub oferującego. Ze wskazanego przepisu ma być usunięte określenie „w szczególności";
- uwagi do art. 1 pkt 63 projektu – **została uwzględniona** poprzez uzupełnienie projektu o rozwiązanie wskazujące maksymalny okres (od ustania przesłanek, o których mowa w projektowanym art. 96 d ust. 3 ustawy o ofercie publicznej) w czasie którego można opublikować dane osobowe, których na podstawie art. 96d ust. 5 przytoczonej ustawy nie przekazano do publicznej wiadomości oraz doprecyzowanie w projekcie przepisów o retencji danych osobowych upublicznianych na stronie internetowej Komisji Nadzoru Finansowego, informacjach związanych z nakładaniem kar pieniężnych, możliwości wykluczenia papierów wartościowych z obrotu oraz nakazu zaprzestania działań skutkujących powstaniem naruszeń.

[164] ZSPU.023.194.2018

Przechowywanie i udostępnianie dokumentów z wyborów

Kolejnym aktem prawnym opiniowanym przez Prezesa UODO był projekt **rozporządzenia Ministra Kultury i Dziedzictwa Narodowego w sprawie sposobu przekazywania, przechowywania i udostępniania dokumentów z wyborów**[165]. W dokumentach z wyborów znajdują się m.in. szczególne kategorie danych osobowych w rozumieniu art. 9 ust. 1 RODO – ujawniające poglądy polityczne i światopoglądowe, a także stan zdrowia wyborców – w ocenie Prezesa UODO istotne jest, by rozporządzenie dotyczące sposobu przekazywania, przechowywania i udostępniania zawierających takie dane nośników w sposób kompletny uregulowało te zagadnienia, rozporządzenie powinno zwierać dodatkowy rozdział dotyczący postępowania z dokumentami z wyborów znajdujących się w Komitetach Wyborczych. W projekcie nie przewidziano przepisów, w jakich przypadkach organ może odmówić wglądu do dokumentów lub dokonania reprodukcji dokumentów. Ponieważ zarówno ustawa, jak i projektowane rozporządzenie, nie wymienia enumeratywnie wszystkich kategorii dokumentów mogących posiadać status „dokumentów z wyborów", procedura ta może więc dotyczyć wglądu do dokumentów zawierających dane osobowe ujawniające poglądy polityczne czy światopoglądowe.

W opinii Prezesa UODO projektowane przepisy powinny zawierać przesłankę do odmowy udostępnienia ww. dokumentów przez dyrektora delegatury Krajowego Biura Wyborczego, w przypadku jeżeli zawarte w nich informacje mogłyby ujawniać szczególne kategorie danych, o których mowa w art. 9 RODO.

1. **projekt ustawy o zmianie ustawy Prawo energetyczne oraz niektórych innych ustaw**[166] **- inteligentne systemy pomiarowe – ocena skutków dla ochrony danych –administrator, decydowanie o celach i sposobach przetwarzania danych - okresy retencji danych - zasada ograniczenia przetwarzania - wyłączenie obowiązków informacyjnych - bezpieczeństwo przetwarzania danych w rejestrach danych - profilowanie odbiorców energii**

Przedmiotem uwag były:

- wprowadzenie systemowego rozwiązania w zakresie inteligentnych systemów pomiarowych – brak analizy, oceny skutków dla ochrony danych osobowych[167];
- przepisy regulujące funkcjonowanie centralnego systemu informacji pomiarowych – powinno z nich wynikać, kto będzie podmiotem decydującym o celach i sposobach przetwarzania danych osobowych w systemie (czy będzie to operator informacji pomiarowych), komu te dane będą przekazywane, w jakich celach oraz w jakim zakresie, jak długo będą przechowywane, na jakiej podstawie, na jakich zasadach i w jaki sposób inne podmioty będą mogły przetwarzać dane osobowe z systemu;
- konieczność wyjaśnienia i uzasadnienia z czego wynikają: trzy i pięcioletni okres przechowywania danych pomiarowych (w pojęciu których mieszczą się także dane osobowe)
- wątpliwości co do propozycji możliwości zlecania przetwarzania danych osobom trzecim przez podmioty, którym jednostkowe dane pomiarowe lub informacje o punkcie pomiarowym są udostępniane, w ich imieniu tych podmiotów;

[165] ZSPU.023.85.2018, (Dz. U. z 2018 r. poz.1995)

[166] ZSPR.023.42.2018.AG; ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2019 r. poz. 755) – dalej: Prawo energetyczne.

[167] Zgodnie z art. 35 ust 1 rozporządzenia 2016/679, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. W myśl zaś art. 35 ust. 4 tego rozporządzenia organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania skutków dla ochrony danych na mocy art. 35 ust. 1 (…).

- zakwestionowanie propozycji wyłączenia w ustawie obowiązków z art. 13 i art. 14 rozporządzenia 2016/679 – niewystarczający powód jakim jest „zbyt duża częstotliwość przetwarzania danych pomiarowych"; ewentualne ograniczenie tych obowiązków może nastąpić jedynie pod pewnymi warunkami, w zgodzie z art. 23 rozporządzenia 2016/679;
- konieczność precyzyjnego określania ról poszczególnych podmiotów, wynikających z rzeczywistych celów i potrzeb związanych z przetwarzaniem danych osobowych – niezbędne dla funkcjonowania projektowanych rozwiązań zgodnie z prawem; przepisy prawa nie muszą wprost wskazywać/nazywać kto jest administratorem, najistotniejsze jest natomiast określenie celów przetwarzania danych osobowych i podmiotu, który o nich decyduje – ról poszczególnych podmiotów w procesie przetwarzania danych osobowych, z uwzględnieniem przepisów rozporządzenia 2016/679;
- obowiązek zdalnego pozyskiwania danych pomiarowych dotyczących każdego odbiorcy końcowego o pobranej z sieci energii za okresy 60 minutowe oraz o wartości mocy za okresy 15 minutowe – może prowadzić do **profilowania**[168] osób będących odbiorcami końcowymi;
- profilowanie ze swej istoty prowadzi do gromadzenia niezwykle złożonego, szczegółowego, potężnego i właściwie trudnego do zmierzenia zasobu informacji, do analizy sytuacji życiowej, rodzinnej, ekonomicznej, zdrowotnej, przyzwyczajeń, zainteresowań, zachowań, wiarygodności, przemieszczania się, przez każdego administratora gromadzącego takie informacje, administratora, który może te informacje wykorzystywać. Istotne jest zatem stworzenie w tym zakresie przepisów, które nie będą naruszać praw osób, których dane dotyczą, czy też prawa te ograniczać; tworzone przepisy prawa powinny gwarantować osobom, których dane dotyczą, ochronę ich praw wynikających z rozporządzenia 2016/679 i innych uregulowań dotyczących ochrony danych osobowych;
- brak alternatywnego rozwiązania dla odbiorców indywidualnych, którzy nie życzą sobie profilowania w zakresie ilości zużywanej energii w przedziałach czasowych doby, czy miesiąca; jeżeli profilowanie ma być stosowane na podstawie przepisów prawa, to przepisy te powinny gwarantować właściwe środki ochrony praw osób, których dane dotyczą;
- przepisy dotyczące rejestru magazynów – zasadność zamieszczania w przedmiotowym rejestrze wszystkich danych, przede wszystkim zaś numer PESEL;
- obowiązek prowadzenia rejestrów przez: Prezesa Urzędu Regulacji Energetyki, właściwych ministrów, Szefów Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu i Centralnego Biura Antykorupcyjnego, ministra właściwego do spraw transportu koniecznym jest – regulacje w tym zakresie powinny gwarantować właściwy poziom bezpieczeństwa przetwarzanych w tych rejestrach danych osobowych.

2. **Zgodność z przepisami rozporządzenia 2016/679 i przeprowadzenie oceny skutków dla ochrony danych osobowych – regulacje prawne w zakresie rachunków bankowych należących do osób zmarłych (tzw. rachunki uśpione)** [169]

Przedmiotem uwag były:

[168] Kwestię profilowania reguluje art. 22 rozporządzenia 2016/679. Przepis ten wskazuje, że osoba, której dane dotyczą, ma prawo nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, chyba że decyzja ta: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewidują właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

[169] DOLIS.035.1260.16.AG

- konieczność określenia w przepisach właściwych procedur, które będą uwzględniały zasady wynikające z rozporządzenia 2016/679;
- konieczność przeprowadzenia oceny skutków dla ochrony danych osobowych.

3. **Teletransmisje w lokalach wyborczych za pośrednictwem publicznie dostępniej sieci elektronicznego przekazywania danych – ustawa o zmianie niektórych ustaw w celu zwiększenia udziału obywateli w procesie wybierania, funkcjonowania i kontrolowania niektórych organów publicznych, zmieniającej m.in. ustawę z dnia 5 stycznia 2011 r. Kodeks wyborczy**[170] (zwaną dalej kodeksem wyborczym)

przepis zakładający teletransmisję z lokalów wyborczych został uchylony.[171]

Przedmiotem uwag były:

- pismo do Państwowej Komisji Wyborczej[172]
- konieczność dostosowania przyjmowanych rozwiązań do przepisów o ochronie danych, w szczególności rozporządzenia 2016/679
- transmisja lub rejestracja z lokalu wyborczego w dniu głosowania może prowadzić do ingerencji w prywatność osób oddających głosy, jak i naruszać tę prywatność – prezentowanie wizerunków, nie tylko twarzy wyborców, ale także zachowania osób biorących udział w głosowaniu
- skutkiem przeprowadzania transmisji lub rejestracji w lokalach wyborczych byłoby także ujawnianie miejsca zamieszkania (lub miejsca pobytu w czasie głosowania) osób oddających głosy
- regulacje prawne powinny precyzyjnie określać zakres danych osobowych oraz cele, dla których będą one przetwarzane oraz być podporządkowane zadaniom nałożonym na podmioty publiczne, aby nie przekraczać kryterium „niezbędności w demokratycznym państwie prawnym".
- nie powinno dochodzić do transmisji czy rejestracji umieszczania przez wyborcę karty do głosowania w urnie; transmisja ukazująca urnę potencjalnie może prowadzić do publicznego ujawnienia tego, w jaki sposób głosował dany wyborca.

4. Tworzenie centralnych rejestrów/systemów teleinformatycznych – zgodność z przepisami rozporządzenia 2016/679, podstawy prawne przetwarzania danych, ochrona danych w fazie projektowania, domyślna ochrona danych – projekt ustawy o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym[173]**,** dotyczące m.in. utworzenia rejestru centralnego – Systemu Rejestracji Broni

Przedmiotem uwag były:

- rozwiązania w zakresie tworzenia/zmiany w systemach teleinformatycznych muszą być zgodne z zasadami ochrony danych osobowych ujętymi w przepisach rozporządzenia 2016/679,
- przy tworzeniu przepisów dedykowanych systemom teleinformatycznym należy uwzględnić ochronę danych w fazie projektowania oraz domyślną ochronę danych oraz ocenę skutków dla ochrony danych;

[170] Ustawa z dnia 5 stycznia 2011 r. – Kodeks wyborczy (Dz. U. z 2019 r. poz. 684) – dalej: Kodeks wyborczy.

[171] Ustawa z dnia 15 czerwca 2018 r. o zmianie ustawy – Kodeks wyborczy oraz niektórych innych ustaw (Dz.U. 2018 r. poz. 1349)..

[172] DOLIS.027.437.2018.AG

[173] ZSPR.023.23.2018; ustawa z dnia 22 czerwca 2001 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2018 r. poz. 2037)

- konieczność dysponowania odpowiednimi podstawami do funkcjonowania systemów informatycznych w przepisach powszechnie obowiązującego prawa o właściwej ich randze.
- konieczność uregulowania zasad przetwarzania danych osobowych w ramach Systemu Rejestracji Broni, w którym to minister będzie decydował o celach i środkach przetwarzania danych osobowych[174].

5. Prowadzenie systemu teleinformatycznego i najważniejszych związanych z tym kwestii w przepisach rangi ustawy – podstawy funkcjonowania systemów teleinformatycznych w przepisach powszechnie obowiązującego prawa o właściwej randze – uwzględnienie ochrony danych w fazie projektowania – ocena skutków dla ochrony danych – projekt rozporządzenia Ministra Środowiska w sprawie wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów[175].

- konieczność uregulowania najważniejszych kwestii związanych z prowadzeniem systemu teleinformatycznego w przepisach rangi ustawy
- podtrzymanie postulatów zgłoszonych w wystąpieniu z dnia 10 maja 2018 r. do Ministra Środowiska dotyczących konieczności wprowadzenia stosownych zmian w ustawie o odpadach, w zakresie konieczności uregulowania w niej najistotniejszych kwestii związanych z funkcjonowaniem monitoringu.[176]

6. projekty aktów prawnych w związku z tworzeniem rejestrów/ewidencji w systemach teleinformatycznych – konieczność dysponowania odpowiednimi podstawami do funkcjonowania systemów teleinformatycznych w przepisach powszechnie obowiązującego prawa o właściwej randze – ochrona danych w fazie projektowania - domyślna ochrona danych – ocena skutków dla ochrony danych

- **rozporządzenie zmieniające rozporządzenie Ministra Finansów w sprawie zaświadczeń o uzyskanej wygranej oraz ewidencji zaświadczeń i ewidencji wypłaconych (wydanych) wygranych**[177]**,**
- **rozporządzenie Ministra Finansów zmieniające rozporządzenie w sprawie dokumentacji prowadzonej przez podmioty prowadzące działalność w zakresie gier hazardowych**[178]**,**
- **rozporządzenie Ministra Finansów zmieniające rozporządzenie w sprawie trybu zgłaszania roszczeń uczestników gier hazardowych**[179]

7. regulowanie zawodów – zakres i cel przetwarzania, podmiot pozyskujący dane, zakres danych w dokumentach – zasada minimalizacji – projekty trzech ustaw: 1) ustawy o architektach, 2) ustawy o inżynierach budownictwa 3) ustawy przepisy wprowadzające ustawę

[174] Projekt skierowano do sejmowej Komisji Administracji i Spraw Wewnętrznych 30 maja 2019 r. (druk nr 3477). Część uwag została uwzględniona.

[175] ZSPR.023.7.2019.AG

[176] Prace legislacyjne nad projektem w okresie sprawozdawczym nie zostały jeszcze zakończone i były na etapie konsultacji międzyresortowych.

[177] ZSPR.023. 43.2018; rozporządzenie Ministra Finansów z dnia 22 czerwca 2010 r. w sprawie zaświadczeń o uzyskanej wygranej oraz ewidencji zaświadczeń i ewidencji wypłaconych (wydanych) wygranych (Dz. U. z 2018 r. poz. 2325).

[178] ZSPR.023.44.2018; rozporządzenie Ministra Finansów z dnia 4 stycznia 2010 r. w sprawie dokumentacji prowadzonej przez podmioty prowadzące działalność w zakresie gier hazardowych (Dz. U. z 2019 r. poz. 26).

[179] ZSPR.023.46.2018; rozporządzenie Ministra Finansów z dnia 2 stycznia 2019 r. w sprawie trybu zgłaszania roszczeń uczestników gier hazardowych (Dz. U. z 2019 r. poz. 20).

o architektach i ustawę o inżynierach budownictwa[180] zakładających odrębne uregulowanie zawodu architekta oraz zawodu inżyniera budownictwa.

- konieczność doprecyzowania proponowanych przepisów o zakres, przez kogo i w jakim celu dane osobowe mają być pozyskiwane – zagrożenie pozyskiwania i gromadzenia danych osobowych w szerszym zakresie niż jest to niezbędne do osiągnięcia celu przez danego administratora
- propozycja obowiązku przedkładania przez kandydatów ubiegających się o tytuł zawodowy architekta/inżyniera budownictwa dokumentów zawierających m.in. lokalizację i nazwę inwestora, u którego kandydaci pełnili funkcje techniczną –inwestorem może być osoba fizyczna, dlatego przepisy powinny – z uwzględnieniem zasady minimalizacji - określać jakie konkretnie dane osobowe takich inwestorów powinny być zamieszczane w przedmiotowej dokumentacji. propozycja utworzenia rejestru ukaranych z tytułu odpowiedzialności dyscyplinarnej członków okręgowej izby inżynierów budownictwa – powinna być w przepisach szczegółowo i kompleksowo uregulowana. Sama wzmianka o fakcie prowadzenia rejestru jest niewystarczająca[181].

8. Zakres danych osobowych we wnioskach – projekt ustawy o zmianie ustawy – Prawo o adwokaturze oraz ustawy o radcach prawnych[182]

- możliwość wydłużenia okresu, przez który aplikant jest wpisany na listę aplikantów po odbyciu aplikacji we wskazanych w projekcie przypadkach, pod warunkiem złożenia przez aplikanta odpowiedniego wniosku – zakres danych we wniosku, jakie dokumenty dołączone mają być do wniosku.
- wydłużenie okresu wpisu na listę aplikantów w związku ze szczególnymi sytuacjami związanymi z chorobą czy macierzyństwem aplikanta - informacje potwierdzające istnienie u poszczególnych aplikantów szczególnych sytuacji takich jak choroba, ciążą etc. będą stanowiły szczególną kategorie danych osobowych w rozumieniu rozporządzenia 2016/679[183]. – regulacje te powinny przewidywać odpowiednie i konkretne środki ochrony podstawowych interesów osoby, której dane dotyczą[184].

9. Cel, zakres i zasady przetwarzania danych przez ministra w rejestrze – projekt ustawy o finansowym wspieraniu produkcji kulturowych gier wideo oraz o zmianie niektórych innych ustaw[185]

- utworzenie rejestru przyznanego wsparcia finansowego produkcji kulturowych gier wideo - jeżeli w rejestrze tym będą gromadzone dane osobowe, to koniecznym jest doprecyzowanie przepisu poprzez wskazanie podmiotu, który prowadzi rejestr (minister)

[180] ZSPR.023.36.2018.AG

[181] Projektodawca do chwili obecnej nie odniósł się do zastrzeżeń Prezesa UODO. Prace legislacyjne nad projektem nie zostały jeszcze zakończone i są na etapie uzgodnień międzyresortowych.

[182] ZSPR.023.45.2018.AG; Projektodawca nie uwzględnił uwag organu nadzorczego. Projekt został skierowany do Sejmu.

[183] Zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. W myśl zaś art. 9 ust 2 lit. g) rozporządzenia 2016/679 ust.1 nie ma zastosowania, jeżeli przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony podstawowych interesów osoby, której dane dotyczą.

[184] Wymogi, o których mowa w art. 9 ust. 2 pkt g rozporządzenia 2016/679.

[185] ZSPR.023.48.2018.AG.

, celu oraz zasad przetwarzania danych przez ministra, okresu przez jaki dane mają być przechowywane, sposobu postępowania z danymi po wygaśnięciu celu przetwarzania, zasad dostępu do tych danych oraz krąg osób czy podmiotów do tego uprawnionych

- wyczerpujące wskazanie (stanowiące zamknięte katalogi) podmiotów, osób, które mają mieć dostęp do danych z rejestru jak i warunków (przesłanek), kiedy to może następować – władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2 Konstytucji RP)[186].

10. Administrator – zadania i kompetencje związane z prowadzeniem rejestru – projekt ustawy o firmach inwestujących w najem nieruchomości[187]

- administratorem danych gromadzonych w rejestrze jest Komisja – brak doprecyzowania w przepisach jakie są zadania czy kompetencje bezpośrednio związane z prowadzeniem przedmiotowego rejestru
- doprecyzowanie zakresu jawnych kategorii danych – adresu zamieszkania oraz numeru PESEL członków zarządu oraz rady nadzorczej firm inwestujących w najem nieruchomości, ale także czynienie tych danych jawnymi – konieczne jest stworzenie regulacji ograniczającej publikowanie danych w zakresie numerów PESEL i adresów ww. osób, tym bardziej, że projektodawca nie wykazał niezbędności ujawniania tych danych dla realizacji celów projektowanej ustawy[188].

Rządowy projekt ustawy o zmianie ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz niektórych innych ustaw.

W opiniowanym przez Generalnego Inspektora Ochrony Danych Osobowych rządowym projekcie ustawy o zmianie ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz niektórych innych ustaw[189] projektodawca regulował gromadzenie danych dotyczące stanu zdrowia, kształcenia, sytuacji, zawodowej i rodzinnej osób, które złożyły wniosek o ustalenie niepełnosprawności albo o ustalenie stopnia niepełnosprawności.

GIODO wskazywał, że zaproponowana zmiana może spowodować, że nie będzie jasne kto (powiatowy zespół, wojewódzki zespół lub Pełnomocnik Rządu do Spraw Osób Niepełnosprawnych) będzie miał dostęp do jakich danych dotyczących stanu zdrowia, kształcenia, sytuacji, zawodowej i rodzinnej osób, które złożyły wniosek o ustalenie niepełnosprawności albo o ustalenie stopnia niepełnosprawności i w jakiej sytuacji (czy w każdej konkretnej sprawie będzie potrzebny tak szeroki zakres danych). Zaproponowane przepisy nie precyzowały w jakim zakresie i w jakim celu będą takie dane przetwarzane oraz czy podmiotom wymienionym w art. 6d ust. 4a ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych również takie dane będą udostępniane. W tym kontekście GIODO wskazał również, że projektodawca nie przeprowadził oceny skutków przetwarzania dla ochrony danych osobowych (art. 35 RODO).

GIODO uznał również za niewystarczający przepis stanowiący o tym, że w warsztacie może działać Rada Społeczna, której zadaniem jest wspieranie warsztatu w realizacji celu działalności tego warsztatu. W przepisie brakowało określenia wyraźnej podstawy prawnej, która będzie umożliwiała przetwarzanie danych przez Radę Społeczną, zakresu danych jakie będą przetwarzane przez członków Rady Społecznej adekwatnych do celu ich przetwarzania, okres czasu przetwarzania oraz dookreślenia warunków udostępniania danych innym podmiotom jeżeli wystąpiłaby taka okoliczność.

---

[186] Projektodawca do chwili obecnej nie odniósł się do uwag Prezesa UODO. Prace legislacyjne nad projektem nie zostały jeszcze zakończone.

[187] DOLiS-023.118/2018 oraz ZSPR.023.118.2018.

[188] Prace nad projektem ustawy o firmach inwestujących w najem nieruchomości nie zostały zakończone w 2018 r. i aktualnie projekt jest na etapie prac w Komisjach Sejmowych (druk 2917). Uwagi UODO uwzględniono.

[189] DOLiS.023.21.2018

GIODO zwrócił uwagę również na brak w projektowanych przepisach dookreślenia zakresu danych osób niepełnosprawnych, których zgłoszenie do uczestnictwa w warsztacie zostało zatwierdzone i które nie rozpoczęły terapii w warsztacie wpisanych do prowadzonej przez warsztat listy oraz konieczność wskazania retencji tych danych.

Projekt ustawy o zmianie ustawy o przeciwdziałaniu narkomanii

Opiniując projekt ustawy o zmianie ustawy o przeciwdziałaniu narkomanii[190], Generalny Inspektor Ochrony Danych Osobowych uznał za niewystarczające określenie tylko w drodze rozporządzenia szczegółowego sposobu gromadzenia, przechowywania i przekazywania informacji w ramach Centralnego Wykazu Osób Objętych Leczeniem Substytucyjnym. GIODO wskazał, że nie ma przeszkód, aby kwestie techniczne związane z przetwarzaniem danych osobowych regulowano w formie aktu wykonawczego. Jednak ważne jest, aby to w przepisach projektowanej ustawy, a nie rozporządzenia, określić zakres danych osobowych przetwarzanych w ramach Centralnego Wykazu Osób Objętych Leczeniem Substytucyjnym, okres ich przechowywania, sposoby ich aktualizacji i usuwania oraz zasady przekazywania takich danych

Rozporządzenie Ministra Zdrowia w sprawie dyspozytorni medycznej

W swojej opinii, zawierającej uwagi do rozporządzenia Ministra Zdrowia w sprawie dyspozytorni medycznej [191]GIODO zakwestionował wprowadzone pojęcie administratora Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, wskazując, że nie jest jasne, jaka rola – w tym jakie działania na danych osobowych – jest przypisywana temu podmiotowi przez projektodawcę. Generalny Inspektor odniósł się również do propozycji rozwiązań dotyczących monitoringu wizyjnego w dyspozytorni, zastosowania kontroli dostępu do pomieszczeń dyspozytorni oraz programu do rejestracji i udostępniania nagrań rozmów prowadzonych przez dyspozytorów medycznych. Wskazał, że powyższe rozwiązania powinny zostać uregulowane w akcie prawnym rangi ustawowej tak, aby nie naruszyć konstytucyjnych praw i wolności.

Projekt ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw

Jednym z projektów opiniowanych przez Prezesa UODO był Projekt ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw**[192].** Projekt ten zakładał utworzenie korpusu kontrolerskiego w centrali Narodowego Funduszu Zdrowia oraz przyznanie Prezesowi NFZ szeregu uprawnień kontrolnych.

Prezes UODO wnioskował o usunięcie przepisów, które nie dają podstaw do kontroli podmiotów, z którymi NFZ nie podpisał umowy o udzielanie świadczeń opieki zdrowotnej. Wskazał na konieczność uzupełnienia przepisów o warunki i zakres współdziałania Prezesa NFZ z podmiotami, które udostępniają mu dane osobowe zawarte w aktach sprawy, zbiorach danych, ewidencjach i rejestrach. Prezes UODO proponował również, aby w ustawie uregulować zakres danych zawartych w legitymacji kontrolerskiej, a także zwrócić szczególną uwagę aby projektowane przepisy zapewniały bezpieczeństwo przekazywanych danych oraz kwestię związaną z zachowaniem tajemnicy kontrolerskiej.

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego w sprawie danych przetwarzanych w Zintegrowanym Systemie Informacji o Szkolnictwie Wyższym i Nauce POL-on

Kolejnym opiniowanym przez Prezesa UODO projektem był projekt Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie danych przetwarzanych w Zintegrowanym Systemie Informacji o Szkolnictwie Wyższym i Nauce POL-on[193]. Projekt zakładał gromadzenie danych z obszaru nauki w jednym spójnym systemie w celu ich ujednolicenia i zachowania przejrzystości.

[190] DOLiS.023.46.2018
[191] DOLiS.023.101.2018
[192] ZSZZS.023.92.2018
[193] ZSZZS.023.48.2018

Prezes UODO sugerował skrócenie 20-letniego okresu przechowywania danych osobowych w poszczególnych wykazach z uwagi na możliwość ich przetwarzania przez okres dłuższy niż jest to niezbędne. Zwrócił również uwagę na brak możliwości usunięcia danych osobowych z bazy oraz na konieczność wprowadzenia okresu retencji danych. Prezes UODO zakwestionował także pozostawienie otwartego dostępu w Systemie POL-on do informacji o prawomocnym orzeczeniu kary dyscyplinarnej, wskazując na to, że ujawnianie takich informacji może prowadzić do pewnego rodzaju naznaczania osób, którym taka kara dyscyplinarna zostanie orzeczona, mając na uwadze, że z projektowanego przepisu nie wynika czy będą publikowane również informacje o wznowieniu postępowania oraz zatarciu takiej kary. Dodatkowo w ocenie Prezesa UODO projektodawca nie przeprowadził oceny skutków dla ochrony danych.

Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej zmieniające rozporządzenie w sprawie przyznania osobie niepełnosprawnej środków na podjęcie działalności gospodarczej, rolniczej albo działalności w formie spółdzielni socjalnej

Odnosząc się do projektu rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej zmieniającego rozporządzenie w sprawie przyznania osobie niepełnosprawnej środków na podjęcie działalności gospodarczej, rolniczej albo działalności w formie spółdzielni socjalnej[194], określającego szczegółowe warunki i tryb przyznawania osobie niepełnosprawnej środków na podjęcie działalności gospodarczej, rolniczej albo działalności w formie spółdzielni socjalnej, Prezes UODO zwrócił uwagę na brak zasadności przetwarzania danych w postaci numeru rachunku bankowego już na etapie składania wniosku. Argumentował to przede wszystkim tym, że złożenie wniosku nie gwarantuje osobie, która go złożyła przyznania środków i zawarcia umowy, ponieważ przepisy rozporządzenia wyraźnie wskazywały, że wniosek ten może zostać negatywnie rozpatrzony przez starostę. W ocenie Prezesa UODO podawanie – już na etapie składania wniosku, numeru tego rachunku jest nieadekwatne do celu przetwarzania.

Wobec powyższego organ ochrony danych osobowych zaproponował usunięcie numeru rachunku bankowego ze wzoru wniosku, wskazując na to, że numer ten będzie potrzebny dopiero na późniejszym etapie, czyli po pozytywnym rozpatrzeniu wniosku, do zawarcia i rozliczenia umowy.

Projekt ustawy o zmianie ustawy – Prawo oświatowe i ustawy o systemie oświaty oraz niektórych innych ustaw

Projekt ustawy o zmianie ustawy – Prawo oświatowe i ustawy o systemie oświaty oraz niektórych innych ustaw[195] zakładał wprowadzenie zmian mających na celu podniesienia atrakcyjności kształcenia w szkołach i placówkach oraz polegających na dostosowywaniu kształcenia do potrzeb rynku pracy.

Prezes UODO zakwestionował w powyższym projekcie przekazywanie kopii umowy, którą dyrektor zawiera z instytucją certyfikującą do ministra koordynatora Zintegrowanego Systemu Kwalifikacji z uwagi na niejasny cel pozyskiwania danych zawartych na tej umowie, tym bardziej, że pozyskiwanie kopii takiej umowy nie wynika z zadań lub obowiązków ministra. Wskazał również, że niezgodne z zasadą minimalizacji danych jest pozostawienie w projekcie sformułowania, które daje możliwość okręgowej komisji egzaminacyjnej przekazywania dyrektorom placówek informacji o egzaminatorach, która nie precyzuje zakresu oraz celu takiej informacji. Ponadto organ wskazał także, że podawanie danych kontaktowych, których obowiązek nie wynika wprost z przepisów ustawy powinno mieć charakter dobrowolny.

Projekt rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie przyznania spółdzielni socjalnej środków na utworzenie stanowiska pracy i finansowanie kosztów wynagrodzenia osób niepełnosprawnych

Prezes UODO opiniował także projekt rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie przyznania spółdzielni socjalnej środków na utworzenie stanowiska pracy i finansowanie

[194] ZSZZS.023.82.2018
[195] ZSZZS.023.26.2018

kosztów wynagrodzenia osób niepełnosprawnych[196]. Projekt regulował możliwość przyznania spółdzielniom socjalnym jednorazowego wsparcia ze środków Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych na utworzenie stanowiska pracy dla skierowanej osoby niepełnosprawnej.

Prezes UODO zakwestionował dołączanie do informacji o kosztach płacy kopii listy płac oraz kopię listy obecności, wskazując, że kopie tych dokumentów mogą zawierać również dane osobowe innych pracowników, których dane osobowe będą w ten sposób ujawnione. Organ zaproponował zrezygnowanie z powyższej praktyki na rzecz odpisów bądź oświadczeń dotyczących konkretnej osoby fizycznej. Wskazał również, że przetwarzanie danych osobowych poręczyciela nie znajduje podstawy prawnej w ustawie o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, a także ocenił, że jednoczesne przetwarzanie numeru PESEL oraz numeru i serii dokumentu potwierdzającego tożsamość za stanowi nadmiarowe przetwarzanie danych osobowych.

Projekt rozporządzenia Ministra Edukacji Narodowej w sprawie wykazu zajęć prowadzonych bezpośrednio z uczniami lub wychowankami albo na ich rzecz przez nauczycieli poradni psychologiczno-pedagogicznych oraz nauczycieli: pedagogów, psychologów, logopedów, terapeutów pedagogicznych i doradców zawodowych

Prezes UODO opiniował także projekt rozporządzenia Ministra Edukacji Narodowej w sprawie wykazu zajęć prowadzonych bezpośrednio z uczniami lub wychowankami albo na ich rzecz przez nauczycieli poradni psychologiczno-pedagogicznych oraz nauczycieli: pedagogów, psychologów, logopedów, terapeutów pedagogicznych i doradców zawodowych [197], który określał zadania realizowane przez nauczycieli w ramach zajęć prowadzonych bezpośrednio z uczniami lub wychowankami, w tym prowadzenia pomocy psychologiczno-pedagogicznej.

Prezes UODO zgłosił uwagi związane z projektowanym prowadzeniem przez nauczycieli poradni psychologiczno-pedagogicznych badań diagnostycznych dzieci i młodzieży oraz podejmowania wobec nich innych działań diagnostycznych, w tym badań przesiewowych. Zwrócił uwagę, że w projekcie nie wskazano zakresu bądź rodzaju badań diagnostycznych i przesiewowych, którym planowane jest poddawanie dzieci i młodzieży, a badania te zgodnie z art. 9 ust. 1 RODO zawierają dane osobowe zaliczane do szczególnych kategorii danych osobowych.

Organ do spraw ochrony danych osobowych sugerował ponowną analizę przepisów prawa z zakresu oświaty i wychowania tak, aby przetwarzanie danych dotyczących zdrowia uczniów lub wychowanków odbywało się zgodnie z przepisami dotyczącymi ochrony danych osobowych, a w szczególności RODO.

Projekt rozporządzenia Ministra Zdrowia w sprawie organizowania, przeprowadzania i dokumentowania badań lekarskich osób ujętych przez funkcjonariuszy Straży Marszałkowskiej

Wątpliwości Prezesa UODO w zakresie projektu rozporządzenia Ministra Zdrowia w sprawie organizowania, przeprowadzania i dokumentowania badań lekarskich osób ujętych przez funkcjonariuszy Straży Marszałkowskiej[198] budził projektowany załącznik nr 1 do przedmiotowego rozporządzenia stanowiący wzór wniosku o przeprowadzenie badania lekarskiego osoby ujętej, w którym wpisuje się m.in. informacje jej stanie zdrowia. W ocenie organu ochrony danych osobowych osoby wskazane w rozporządzeniu nie posiadają kwalifikacji medycznych do stwierdzenia stanu zdrowia osoby ujętej.

Wobec powyższej argumentacji organ sugerował usunięcie z załącznika nr 1 informacji o stanie zdrowia, z uwagi na wskazanie celu badania lekarskiego oraz późniejsze wydanie zaświadczenia lekarskiego przez lekarza po przeprowadzeniu badania lekarskiego.

Projekt ustawy o zmianie ustawy o Służbie Więziennej oraz niektórych innych ustaw

[196] ZSZZS.023.115.2018
[197] ZSZZS.023.7.2018
[198] ZSZZS.023.2.2018

W związku z projektem ustawy o zmianie ustawy o Służbie Więziennej oraz niektórych innych ustaw[199], Prezes UODO wnioskował o stworzenie zamkniętego katalogu danych, które będą wymagane przy tworzeniu miesięcznego zestawienia, na podstawie którego świadczeniodawca będzie otrzymywał środki publiczne za udzielone świadczenia, co spowodowałoby, że świadczeniodawca nie będzie mógł przekazywać w przedmiotowym zestawieniu innych danych niż te wskazane enumeratywnie w przepisie.

Prezes UODO odniósł się również do propozycji uregulowania oceny predyspozycji do pełnienia służby w kontyngencie. Uznał, że w przedmiotowym przepisie jak i przepisach następnych brak było kryteriów oceny predyspozycji. Z przepisów jasno nie wynikało czy ocena predyspozycji będzie polegała na przeprowadzeniu testu sprawności fizycznej lub badań psychologicznych, czy też będzie to jedynie subiektywna ocena Dyrektora Generalnego lub z jego upoważnienia Komendanta Centralnego Ośrodka Szkolenia Służby Więziennej. W związku z powyższym organ nadzorczy sugerował doprecyzowanie powyższej materii tak, aby zaprojektowany przepis był jasny i nie stanowił problemów interpretacyjnych dla jego adresatów.

7. Zgłaszanie naruszeń ochrony danych osobowych

Kolejnym nowym zadaniem Urzędu realizowanym od 25 maja 2018 r. stało się przyjmowanie od administratorów zgłoszeń naruszeń o ochronie danych osobowych, które stwarzają ryzyko naruszenia praw lub wolności osób fizycznych. Do tej pory obowiązek ten ciążył wyłącznie na administratorach z sektora telekomunikacyjnego. Uzyskanie przez organ nadzorczy informacji o danym naruszeniu ochrony danych osobowych pozwala mu na reakcję i może doprowadzić do ograniczenia skutków takiego naruszenia, co przekłada się na zwiększenie poziomu ochrony praw i wolności osób, których dane dotyczą.

Zgodnie z art. 33 ust. 1 RODO w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Żeby zapewnić należyte wywiązanie się z tego obowiązku przez administratorów, Urząd przygotował formularz zgłoszeniowy, który umożliwia każdemu administratorowi nie tylko przekazanie wszystkich niezbędnych informacji określonych w RODO, ale także podanie dodatkowych danych umożliwiających organowi nadzorczemu dokonanie analizy naruszenia pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Dotychczasowa praktyka wskazuje, że w przypadku administratorów zgłaszających naruszenia na zaproponowanym formularzu, ryzyko przekazania niewystarczających informacji, o których mowa w przepisach jest mniejsze, niż w przypadku naruszeń przesyłanych przez administratorów bez użycia ww. formularza.

Zgłaszanie naruszeń przez administratorów stanowi skuteczne narzędzie przyczyniające się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych. Zgłaszając naruszenie organowi nadzorczemu, administratorzy informują Prezesa UODO, czy w ich ocenie wystąpiło wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą oraz – jeśli takie ryzyko wystąpiło – to czy przekazali stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ.

[199] ZSZZS.023.117.2018

W uzasadnionych przypadkach mogą również przekazać informację, że powiadomienie w ich ocenie nie jest konieczne ze względu na spełnienie warunków określonych w art. 34 ust. 3 lit. a i b RODO. Prezes UODO dokonuje weryfikacji oceny dokonanej przez administratora i może – jeżeli administrator nie zawiadomił osoby – zażądać od niego takiego zawiadomienia. Zawiadomienie osób fizycznych o naruszeniu **zapewnia administratorowi możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie osoby te mogą podjąć, aby uchronić się przed potencjalnymi skutkami naruszenia.** Każdy plan reagowania na naruszenia powinien koncentrować się przede wszystkim na zapewnieniu ochrony osobom fizycznym i ich danym osobowym.

Od 25 maja do 31 grudnia 2018 r. UODO dokonał analizy 2 446 zgłoszeń naruszeń pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w tym **1 882** naruszeń zostało zgłoszonych przez podmioty sektora prywatnego, zaś **564** przez podmioty sektora publicznego. W przypadku sektora prywatnego najwięcej zgłoszeń napłynęło od firm: telekomunikacyjnych, ubezpieczeniowych, finansowych, banków oraz służby zdrowia. W sektorze publicznym zawiadomienia o incydentach z danymi osobowymi najczęściej nadsyłały jednostki samorządu terytorialnego, szkoły, przedszkola, żłobki oraz placówki służby zdrowia.

W celu wyeliminowania nieprawidłowości podjął następujące działania:

- wykonano ok. **700 rozmów telefonicznych** oraz wysłano **120 e-maili** do administratorów i inspektorów ochrony danych – z uwagi na konieczność podejmowania przez organ nadzorczy szybkich działań mających na celu ochronę praw lub wolności osób fizycznych oraz z uwagi na fakt, że do zgłaszania naruszeń nie mają zastosowania przepisy kodeksu postępowania administracyjnego;
- skierowano do administratorów ok. **400 wezwań dotyczących złożenia wyjaśnień** w zakresie nadesłanych zgłoszeń naruszeń – wezwania były kierowane do administratorów w sytuacji, gdy zgłoszone naruszenia ochrony danych osobowych nie zawierały informacji, niezbędnych do oceny naruszenia na podstawie art. 34 ust. 1 i 2 RODO, a kontakt z IOD lub innym punktem kontaktowym był utrudniony;
- skierowano do administratorów **250 wystąpień** – zgodnie z art. 34 ust. 4 RODO „jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać (…)". Wystąpienia nie tylko nakazują zawiadomienie lub ponowne prawidłowe zawiadomienie osób, których dane dotyczą o naruszeniu, ale także spełniały walor edukacyjny jak np. wskazówki dotyczące prawidłowego zawiadomienia osób, których dane dotyczą o naruszeniu;
- wydano **13 decyzji administracyjnych** nakazujących administratorowi zawiadomienie lub ponowne prawidłowe zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych.

W okresie sprawozdawczym wśród zgłoszeń naruszeń ochrony danych osobowych najczęściej popełniane błędy obejmowały:

1) **brak w przesyłanych zgłoszeniach naruszeń, niektórych wymaganych w art. 33 ust. 3 RODO informacji, jak np.**:

- opisu charakteru naruszenia ochrony danych osobowych – w tym w miarę możliwości wskazywanie kategorii i przybliżonej liczby osób oraz wpisów danych osobowych, których dotyczy naruszenie;
- imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisu możliwych konsekwencji naruszenia ochrony danych osobowych;
- opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosowanych przypadkach środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;

2) niedokładne wypełnianie zgłoszeń – w wielu przypadkach informacje przekazywane przez administratorów w zgłoszeniu były lakoniczne i nierzetelne. Brak dokładnego opisu zaistniałego incydentu niejednokrotnie uniemożliwiał ocenę prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Jednym z najważniejszych celów zgłaszania naruszeń ochrony danych jest ograniczenie szkód dla osób fizycznych. Uzyskanie przez organ nadzorczy pełnych, wymaganych w art. 33 ust. 3 RODO informacji o określonym naruszeniu, pozwala mu na właściwą ocenę naruszenia i odpowiednią reakcję polegającą np. na zażądaniu od administratora powiadomienia osób;
3) wypełnianie zgłoszeń w sposób rutynowy, prowadzący do błędów – w przypadku administratorów kierujących do urzędu znaczną ilości zgłoszeń naruszeń, zauważalna była tendencja do niedbałego i szablonowego sposobu wypełniania formularza zgłoszenia naruszenia. To powodowało, że w zgłoszeniach od tych administratorów często obecne były błędy wynikające z automatycznego przenoszenia informacji dotyczących innych zdarzeń, np. wcześniej zgłoszonych naruszeń. Takie błędne, nieścisłe przekazywanie informacji powoduje konieczność prowadzenia z administratorem dalszej korespondencji lub innej formy kontaktu, a tym samym ponoszenia niepotrzebnych nakładów czasu i pracy zarówno po stronie administratora, jak i organu nadzorczego;
4) zgłaszanie naruszeń ochrony danych osobowych przez podmiot przetwarzający bądź inny podmiot nie będący administratorem zobowiązanym do zgłoszenia naruszenia – podmiot przetwarzający nie zgłasza naruszeń ochrony danych osobowych organowi nadzorczemu. Obowiązek ten ciąży na administratorze. W związku z powyższym podmiot przetwarzający powinien niezwłocznie powiadomić administratora o zaistniałym zdarzeniu. Administrator po uzyskaniu niezbędnych informacji jest zobowiązany dokonać analizy i podjąć decyzję o ewentualnym zgłoszeniu naruszenia Prezesowi UODO.

Wśród spraw, które wymagały podjęcia przez Prezesa UODO czynności wobec administratorów w celu doprowadzenia do prawidłowego wykonania obowiązku określonego w art. 34 rozporządzenia 2016/679 w formie decyzji administracyjnej wskazać można na:

- *zgłoszenie naruszenia ochrony danych osobowych polegające na wysłaniu niewłaściwemu klientowi zamówienia (zdjęć) innej klientki administratora*. Spółka oświadczyła w zgłoszeniu, że zamówienie zawiera rodzinne i ciążowe zdjęcia osoby, której dotyczy naruszenie, oraz że w środku koperty, oprócz zdjęć była etykieta właściwego adresata zamówienia. Zgodnie ze zgłoszeniem naruszenie dotyczyło następujących danych osobowych: imię i nazwisko klientki, numer zamówienia, dane jednej z osób widniejącej na zdjęciu w zakresie: imię i nazwisko, data urodzenia, płeć oraz wizerunki klientki i członków jej rodziny, przyjaciół oraz dziecka (w okresie od narodzin do 3. roku życia) z życia codziennego, spotkań rodzinnych oraz innych wydarzeń, m.in.: chrztu, zawarte na 126 zdjęciach.

Ponadto administrator wskazał w zgłoszeniu naruszenia, że zdarzenie dotyczyło danych szczególnych kategorii, tj. danych dotyczących zdrowia oraz danych o przekonaniach religijnych i światopoglądowych. Administrator zrezygnował z zawiadomienia klientki o zdarzeniu, w trybie wskazanym w art. 34 RODO. Prezes UODO skierował do administratora wystąpienie, w którym wezwał do zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych oraz przekazania tej osobie zaleceń odnośnie zminimalizowania potencjalnych negatywnych skutków zaistniałego naruszenia. Administrator w swojej odpowiedzi na wystąpienie wskazał, że nie zawiadomi osoby o zdarzeniu, gdyż na podstawie przytoczonej w piśmie argumentacji nie ocenia ryzyka naruszenia praw lub wolności klientki jako wysokiego.

W ocenie Prezesa UODO ujawnienie osobie nieuprawnionej imienia i nazwiska klientki, danych kontaktowych wraz z miejscem zamieszkania klientki i jej małoletniego dziecka oraz innymi informacjami ujawnionymi na fotografiach przedstawiających sytuacje z życia rodziny w okresie od narodzin dziecka do 3. roku życia dziecka, w tym szczególnych kategorii danych, tj. danych dotyczących zdrowia oraz danych o przekonaniach religijnych i światopoglądowych, powoduje wysokie

ryzyko naruszenia praw i wolności osób fizycznych, a administrator zobowiązany był bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o takim naruszeniu.

Organ nadzorczy wskazał, że ujawnienie takich danych może prowadzić do wyłudzenia środków finansowych od najbliższej rodziny tzw. „metodą na wnuczka", udostępnienia danych lokalizacyjnych dziecka, co może skutkować narażeniem jego bezpieczeństwa oraz prowadzić do dyskryminacji dziecka i jego rodziny, poprzez ujawnienie szczególnej kategorii danych, tj. stanu zdrowia dziecka. Fotografie będące szczególnym nośnikiem informacji, mogą ujawniać wiele cech fizycznych, fizjologicznych, ekonomicznych, kulturowych lub społecznych. Zarówno zdjęcia kobiety w ciąży, jak i utrwalone na fotografiach wydarzenia (okres ciąży, narodziny dziecka, jego chrzest) mogły dotyczyć szczególnej sfery prywatności klientki, intymnych aspektów jej życia i dostęp do takich informacji nie powinny mieć osoby nieuprawnione mogące wykorzystać te informacje w sposób prowadzący do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych lub dyskryminacji. Ponadto Prezes UODO odniósł się do zastosowanej przez administratora procedury oceny naruszenia wdrożonej na podstawie zaleceń Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, wskazując na nieprawidłowe zastosowanie metodologii w przedmiotowym stanie faktycznym i nieuwzględnienie wszystkich okoliczności naruszenia co przełożyło się na błędną ocenę ryzyka naruszenia praw lub wolności.

- *zgłoszenie naruszenia ochrony danych osobowych dotyczące jednego klienta firmy Y* (zgłoszenie dotyczyło takich kategorii danych osobowych jak: numer PESEL, imię, nazwisko, adres zamieszkania, numer telefonu, adres e-mail oraz dane dotyczące pojazdu). *Naruszenie polegało na przesłaniu polisy ubezpieczeniowej na niewłaściwy adres e-mail w związku z czym osoba trzecia mogła się zapoznać z danymi klienta*. Opisywany stan faktyczny dotyczył 16 zgłoszeń naruszeń danego administratora. We wszystkich sprawach firma Y podważała stanowisko organu nadzorczego w sprawie konieczności zawiadomienia osób, których dane dotyczą.

W powyższych sprawach Prezes UODO wszczął postępowania administracyjne, zakończone decyzją nakazującą prawidłowe zawiadomienie osób, które dane dotyczą, zgodnie z art. 34 ust. 2 RODO. W uzasadnieniu decyzji wskazał, że art. 34 ust. 1 i 2 RODO ma na celu nie tylko zapewnienie możliwie najskuteczniejszej ochrony podstawowych praw i wolności podmiotów danych, ale także realizację zasady przejrzystości, która wynika z przepisu art. 5 ust. 1 lit. a RODO. Właściwe wywiązanie się z obowiązku określonego w tym przepisie ma zapewnić osobie, której dane dotyczą – szybko i w sposób przejrzysty informację o naruszeniu ochrony jej danych osobowych wraz z opisem możliwych konsekwencji naruszenia ochrony danych osobowych oraz środków, które może ona podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków. Postępujący zgodnie z prawem i wykazujący dbałość o interesy osoby, której dane dotyczą, administrator powinien zatem bez zbędnej zwłoki zapewnić, osobie, której dane dotyczą, możliwość jak najlepszej ochrony jej praw i wolności wystawionych na ryzyko wynikające z naruszenia ochrony danych osobowych. Dla osiągniecia tego celu konieczne jest przynajmniej wskazanie m.in. tych informacji, które wymienione są w art. 34 ust. 2 w związku z art. 33 ust. 3 RODO, z którego to obowiązku administrator się nie wywiązał.

Zakres przedmiotowy naruszeń ochrony danych osobowych zgłaszanych przez administratorów z sektora publicznego obejmuje najczęściej nieprawidłowości w przetwarzaniu danych osobowych, które można zdefiniować jako:

1) udostępnienie danych osoby innej, niż adresat korespondencji – nieprawidłowo zaadresowana korespondencja (w formie tradycyjnej i za pomocą email) – w tym przypadku naruszenia powstawały wskutek błędu pracowników, miały one charakter incydentalny. Administratorzy podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia, dokonywali przeglądu procedur, wykonywali audyty bezpieczeństwa;

2) udostępnienie danych w trybie dostępu do informacji publicznej, w wyniku nieprawidłowej anonimizacji danych, w tym w Biuletynie Informacji Publicznej – podobnie jak wyżej, naruszenia powstawały wskutek niedopatrzenia pracowników zajmujących się anonimizacją danych.

Administratorzy dokonywali przeglądu procedur oraz deklarowali wprowadzenie dodatkowych procedur np. dodatkowe sprawdzanie dokumentów przez innego pracownika pod kątem anonimizacji dokumentów;

3) zniszczenie/zagubienie/kradzież dokumentacji bądź innych nośników (telefon) zawierających dane osobowe – w tej kategorii można wyróżnić naruszenia polegające na zagubieniu korespondencji przez operatora pocztowego. Administratorzy podejmowali działania mające na celu ustalenie przyczyn zagubienia korespondencji czy weryfikacje umów zawartych z operatorem pocztowym. Należy jednocześnie wskazać, że dochodziło również do kradzieży nośników elektronicznych lub dokumentów zawierających dane osobowe. Administratorzy zgłaszali zdarzenia organom ścigania;

4) naruszenia związane z udostepnieniem danych osobowych osobie nieuprawnionej – w tym przypadku do naruszenia dochodziło wskutek wydawania dokumentów (np. zaświadczeń) petentom urzędów, który zawierały dane osobowe innych osób. Najczęściej naruszenia wynikały z błędów pracowników urzędów. Administratorzy podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia, dokonywali przeglądu procedur, a ponadto zobowiązywali osoby nieuprawnione, które weszły w posiadanie tych dokumentów do ich zwrotu;

5) naruszenia polegające na złamaniu zabezpieczeń systemu informatycznego, które skutkowało zablokowaniem dostępu do plików, całego komputera lub wewnętrznej sieci intranetowej przez złośliwe oprogramowanie typu ransomware – ransomware to rodzaj złośliwego oprogramowania, które szyfruje dane uniemożliwiając do nich dostęp, oferując następnie klucz deszyfrujący za opłatą (spełnienie żądania szantażu nie zawsze spowoduje odszyfrowanie danych). Z reguły charakter taki ma działanie zewnętrzne zamierzone. Administratorzy odzyskiwali dostęp do danych na podstawie kopii zapasowych baz danych wykonywanych automatycznie.

Informacje dotyczące najczęściej zgłaszanych naruszeń w sektorze prywatnym to:

1) dane osobowe wysłane do niewłaściwego odbiorcy (np.: faktura VAT bądź umowa ubezpieczenia pocztą elektroniczną trafiła do innego abonenta, np. wskutek zbieżności nazwisk; na skutek omyłki pracowników przy wpisywaniu adresu e-mail , bądź pracowników podmiotów zewnętrznych – działania niezamierzone; np. klientka podała niewłaściwy adres e-mail na których chciała przesłania dokumentów);

2) luka bezpieczeństwa w systemie informatycznym pozwalająca na uzyskanie nieuprawnionego dostępu do danych osobowych;

3) wysyłka e-maila do wielu adresatów zawierającego e-maile innych adresatów (np.: wskutek wpisania w rubryce „do wiadomości"), wskutek czego osoby niepowołane mogą dowiedzieć się o miejscu pracy lub podmiocie gospodarczym zatrudniającym inne osoby;

4) niezamierzona publikacja danych osobowych na stronie internetowej administratora;

5) przesłanie newslettera z błędnie skonstruowanego skryptu adresów e-mail do wszystkich odbiorców newslettera wraz z linkiem umożliwiającym usunięcie się z bazy;

6) luka bezpieczeństwa pozwalająca na uzyskanie dostępu do danych osobowych innego użytkownika przy logowaniu się do konta billingowego;

7) utracenie przez podmiot umowy z klientem i możliwość wejścia w jego posiadanie przez inny podmiot;

8) omyłkowe udostępnienie w trakcie rozmowy tel. danych innego klienta przez pracownika call center;

9) zagubienie/kradzież niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych – smartfony, komputery przenośne, dyski zewnętrzne;

10) zagubienie dokumentacji papierowej zawierającej dane osobowe (np. list dłużników) przez doradców finansowych w trakcie wyjazdów do klientów;

11) ataki hackerskie mające na celu uzyskanie nieuprawnionego dostępu do bazy danych klientów sklepów internetowych w celu wysyłki phishingowych wiadomości SMS i wyłudzenia danych dostępowych do konta bankowego.

Działania podjęte przez organ nadzorczy w zakresie zgłaszanych przez administratorów incydentów mają w szczególności na celu monitorowanie, zapobieganie oraz reagowanie na przypadki naruszeń mogących skutkować wysokim ryzykiem. Zarówno dla administratorów, jak i dla organu nadzorczego ważnym wydaje się wypracowanie praktyk pozwalających na zmniejszenie liczby incydentów, a co za tym idzie podwyższenie standardów ochrony praw osób, których dane dotyczą.

8. Uprzednie konsultacje

Od 2018 r. do nowych zadań UODO należy również udzielanie zaleceń na wniosek o uprzednie konsultacje złożony przez administratora. Uprzednie konsultacje są narzędziem służącym do współpracy pomiędzy organem nadzorczym oraz administratorem, a ich celem jest jak najlepsze zabezpieczenie operacji przetwarzania danych osobowych. Z wnioskiem o uprzednie konsultacje należy wystąpić w sytuacji, w której w wyniku przeprowadzonej oceny skutków dla ochrony danych na liście badanych operacji przetwarzania znajdą się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i gdy administrator nie może znaleźć środków wystarczających do zmniejszenia (zminimalizowania) tego ryzyka do dopuszczalnego poziomu.

W omawianym okresie sprawozdawczym administratorzy w małym zakresie korzystali z tej formy współpracy z organem nadzorczym – do Urzędu wpłynęły dwa wnioski o przeprowadzenie uprzednich konsultacji. Wnioski te dotyczyły planowanych procesów przetwarzania danych osobowych w ramach wdrażania projektu systemu teleinformatycznego mającego wspomagać realizację zadań jednostek organizacyjnych samorządu terytorialnego oraz obsługę korzystających z ich usług mieszkańców.

Powyższe wnioski nie spełniały jednak wymogów określonych w przepisach o ochronie danych osobowych (były obarczone brakami formalnymi), w związku z powyższym Prezes UODO poinformował wnioskodawcę o nieudzieleniu konsultacji i wskazał przyczyny ich nieudzielenia.

W kilku przypadkach Prezes UODO spotkał się ponadto z nieprawidłowym rozumieniem tej instytucji przez administratorów, powołując się bowiem na tryb uprzednich konsultacji zwracali się oni w istocie z pytaniami prawnymi.

9. Kodeksy postępowania

W 2018 r. w ramach realizacji zadania z art. 57 ust. 1 lit. m RODO, zgodnie z którym organ nadzorczy zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1 RODO, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia na mocy art. 40 ust. ust. 5. Prezes i pracownicy UODO zachęcali do sporządzania kodeksów postępowania określonych w art. 40 RODO podczas szkoleń i spotkań z administratorami i inspektorami ochrony danych oraz w artykułach prasowych. Wyłącznie w tym celu przeprowadzono także dwa warsztaty dla podmiotów zainteresowanych stworzeniem tego narzędzia wykazywania zgodności z zasadami ochrony danych oraz spotkania indywidualne ze zrzeszeniami administratorów.

Pierwsze warsztaty odbyły się 11 stycznia 2018 r.[200]. Był adresowany do organizacji skupiających administratorów reprezentujących różne sektory, które przygotowują się do stosowania przepisów

[200] https://uodo.gov.pl/pl/180/374

ogólnego rozporządzenia o ochronie danych (RODO). W trakcie spotkania reprezentanci branży bankowej, internetowej, biobanków oraz uczelni medycznych przedstawili specyfikę funkcjonowania swoich sektorów. Pracownicy Biura GIODO przedstawili główne założenia przyjmowania kodeksów – treść, elementy składowe oraz procedurę zatwierdzania. W spotkaniu wzięło udział ok. 140 osób.

Drugie warsztaty odbył się 19 września 2018 r.[201] Jego celem było omówienie: zasad, jakich należy przestrzegać, tworząc kodeksy postępowania; jakie podmioty mogą monitorować zatwierdzone kodeksy; w jaki sposób prawidłowo przeprowadzić konsultacje podczas prac nad takimi dokumentami. W spotkaniu wzięli udział przedstawiciele 15 organizacji.

W 2018 r. odbyły się 23 indywidualne spotkania informacyjne dla autorów kodeksów, podczas których przedstawiciele Urzędu informowali o wymogach praktycznych tworzenia kodeksu, a autorzy o rozważanych kierunkach i koncepcjach regulacji kodeksowych. Posłużyły one także poznaniu specyfiki obszarów działalności branż, które mają być doregulowane. Po zakończeniu spotkań część projektodawców wstrzymała dalsze prace nad projektami do czasu ustalenia jednolitej wykładni przepisów RODO dot. kodeksów przez Europejską Radę Ochrony Danych.

UODO prowadzi konsultacje treści kodeksów postępowania przed rozpoczęciem formalnej procedury ich zaopiniowania i zatwierdzenia przez Prezesa UODO.

W 2018 r. trzy organizacje złożyły wnioski o zatwierdzenie projektów kodeksów:

- Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie – Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych,
- Związek Banków Polskich – Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe,
- Polska Federacja Szpitali – kodeks postępowania dla sektora ochrony zdrowia wydany zgodnie z art. 40 RODO dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających.

Pracownicy UODO spotykali się z autorami projektów kodeksów, aby omówić poszczególne postanowienia, oceny sprawozdania z konsultacji i innych elementów wniosku. Dużym wyzwaniem dla podmiotów zrzeszonych jest przyjęcie modelu monitorowania kodeksu, który będzie akceptowalny dla członków z punktu widzenia organizacji działalności i jej finansowania. Należy podkreślić, że skuteczny system monitorowania wiąże się z ponoszeniem kosztów, które zapewnią efektywną kontrolę podmiotów objętych kodeksem, zarówno okresową, jak i nadzwyczajną, w przypadku wystąpienia naruszeń.

W ramach podgrupy eksperckiej Compliance, E-gov, Health, Europejskiej Rady Ochrony Danych przedstawiciele Prezesa UODO uczestniczyli w przygotowaniu Wytycznych 1/2019 w sprawie kodeksów postępowania i podmiotów monitorujących na mocy rozporządzenia 2016/679[202], które były konsultowane publicznie w kolejnym roku. Zatwierdzone wytyczne mają dostarczyć wsparcia interpretacyjnego i praktycznych wskazówek dotyczących przepisów o kodeksach w RODO. Wyjaśniają zasady i procedury związane z przygotowaniem, zatwierdzeniem i publikacją kodeksów na poziomie krajowym i europejskim. Podejście takie ma na celu zapewnienie spójności na poziomie całej Unii Europejskiej i przejrzystości działań podejmowanych przez krajowe organy ochrony danych osobowych w związku z tworzeniem kodeksów. Uzgodnione przez organy ochrony danych kryteria umożliwią rozpatrywanie wniosków o akredytację podmiotów monitorujących.

[201] https://uodo.gov.pl/pl/138/536
[202] https://uodo.gov.pl/pl/138/732

10. Ochrona danych osobowych w kościołach i związkach wyznaniowych

Od 25 maja 2018 r. kościoły lub związki wyznaniowe są zobowiązane do przestrzegania ogólnego rozporządzenia o ochronie danych (RODO). Jednak te kościoły lub związki wyznaniowe, które w momencie wejścia w życie RODO, stosowały już wewnętrzne zasady ochrony danych osobowych, zgodnie z art. 91 ust. 1 RODO mają dalszą możliwość stosowania autonomicznych, szczegółowych regulacji w tym zakresie. Te regulacje muszą być jedynie dostosowane do RODO.

RODO w ten sposób daje możliwość poszanowania autonomii kościołów i związków wyznaniowych o uregulowanym statusie prawnym w RP. W świetle motywu 165 preambuły do RODO, rozporządzenie nie narusza statusu przyznanego kościołom oraz związkom lub wspólnotom wyznaniowym na mocy prawa konstytucyjnego obowiązującego w państwach członkowskich.

W konsekwencji, po 25 maja 2018 r. następujące kościoły lub związki wyznaniowe poinformowały Prezesa UODO bezpośrednio lub za pośrednictwem rządu RP o stosowaniu odrębnych szczegółowych regulacji o ochronie danych osobowych:

- Kościół katolicki,
- Polski Autokefaliczny Kościół Prawosławny,
- Kościół Adwentystów Dnia Siódmego w Rzeczypospolitej Polskiej,
- Kościół Ewangelicko-Augsburski,
- Kościół Ewangelicko-Reformowany w RP,
- Kościół Boży w Polsce z siedzibą w Krakowie,
- Społeczność Chrześcijańska Miejsce Odnowienia z siedzibą w Lublinie,
- Wspólnota Chrześcijańska „Wrocław dla Jezusa" z siedzibą we Wrocławiu,
- Kościół Pentekostalny w Rzeczpospolitej z siedzibą w Żorach,
- Zbór Ewangelicko-Baptystycznego z siedzibą w Katowicach,
- Misja Pokoleń z siedzibą w Krakowie,
- Ewangeliczny Kościół Metodystyczny z siedzibą w Krakowie,
- Powszechny Kościół Ludu Bożego z siedzibą w Jarocinie,
- Kościół „Chrystus dla Wszystkich" w Rzeczypospolitej Polskiej z siedzibą w Szczecinie,
- Kościół Chrześcijan Baptystów w Rzeczypospolitej Polskiej.

Przykładem takich szczegółowych zasad ochrony danych osobowych jest Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim, wydany na podstawie kan. 455 Kodeksu Prawa Kanonicznego przez Konferencję Episkopatu Polski 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie.

Kościół lub związek wyznaniowy, który nie stosuje wskazanych w art. 91 RODO szczegółowych zasad ochrony danych musi w pełni przestrzegać postanowień RODO. Jeżeli kościoły lub związki wyznaniowe, które stosują autonomiczne regulacje o ochronie danych osobowych, prowadzą także działalność regulowaną prawem państwowym, to do niej stosuje się bezpośrednio RODO. Dotyczy to np. przetwarzania danych przez prowadzone przez kościoły lub związki wyznaniowe szkoły działające na prawach szkół publicznych, czy przez podmioty mające status organizacji pożytku publicznego, domy pomocy itp. Tak samo będzie gdy podmioty kościelne będą przetwarzały dane osobowe w kontekście prowadzenia działalności gospodarczej.

Warto dodać, że RODO m.in. daje kościołom lub związkom wyznaniowym możliwość przetwarzania szczególnych kategorii danych, do których, zgodnie z art. 9 RODO, zalicza się dane dotyczące przekonań religijnych. W myśl art. 9 ust. 2 lit. d RODO jest to dopuszczalne w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach religijnych, pod warunkiem że przetwarzanie

dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą.

Zgodnie z art. 91 ust. 2 RODO, kościoły lub związki wyznaniowe, które stosują szczegółowe zasady ochrony danych osobowych, podlegają nadzorowi niezależnego organu nadzorczego, który może być organem odrębnym, ale nie musi to być Prezes UODO.

Po 25 maja 2018 r. Prezes UODO został poinformowany bezpośrednio lub za pośrednictwem rządu o wyznaczeniu następujących niezależnych organów nadzorczych:

- Kościelny Inspektor Ochrony Danych powołany przez Kościół katolicki,
- Kościelny Inspektor Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego,
- Kurator Ochrony Danych Osobowych Kościoła Adwentystów Dnia Siódmego w Rzeczypospolitej Polskiej,
- Ewangelicka Komisja Wspólna Ochrony Danych Osobowych powołana przez Kościół Ewangelicko-Augsburski i Kościół Ewangelicko-Reformowany w RP,
- Inspektor Danych Osobowych powołany przez Kościół Chrześcijan Baptystów w RP,
- Międzykościelna Komisja Ochrony Danych Osobowych, utworzona przez:

– Kościół Boży w Polsce z siedzibą w Krakowie,
– Społeczność Chrześcijańska Miejsce Odnowienia z siedzibą w Lublinie,
– Wspólnotę Chrześcijańską „Wrocław dla Jezusa" z siedzibą we Wrocławiu,
– Kościół Pentekostalny w Rzeczpospolitej z siedzibą w Żorach,
– Zbór Ewangelicko-Baptystycznego z siedzibą w Katowicach,
– Misję Pokoleń z siedzibą w Krakowie,
– Ewangeliczny Kościół Metodystyczny z siedzibą w Krakowie,
– Powszechny Kościół Ludu Bożego z siedzibą w Jarocinie,
– Kościół „Chrystus dla Wszystkich" w Rzeczypospolitej Polskiej z siedzibą w Szczecinie.

Przetwarzanie danych w kościołach lub związkach wyznaniowych, które nie stosują autonomicznych regulacji w zakresie ochrony danych osobowych podlega nadzorowi Prezesa UODO. Nadzorowi Prezesa UODO podlegają także te obszary przetwarzania danych, do których bezpośrednio stosuje się RODO.

Artykuł 59 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych przewiduje współpracę Prezesa UODO z niezależnymi organami nadzorczymi powołanymi na podstawie art. 91 RODO. Polski ustawodawca przewidział także możliwość zawierania przez Prezesa UODO porozumień o współpracy i wzajemnym przekazywaniu informacji z tymi organami nadzorczymi.

Prezes UODO wspiera wszelkie działania mające na celu zwiększanie świadomości w zakresie ochrony danych osobowych w kościołach i związkach wyznaniowych. Jedną z takich inicjatyw było objęcie przez Prezesa UODO patronatem honorowym prowadzonych na Uniwersytecie Kardynała Wyszyńskiego w Warszawie studiów podyplomowych poświęconych ochronie danych osobowych w Kościele.

Członkowie kościołów lub związków wyznaniowych powinni być informowani o swoich prawach związanych z przetwarzaniem danych osobowych. Służą im również pozostałe prawa gwarantowane przez RODO. W sytuacjach objętych nadzorem przez kościelne organy nadzorcze takim osobom służy skarga do nich.

11. 20 lat rejestracji zbiorów danych osobowych

Generalny Inspektor Ochrony Danych Osobowych (GIODO) prowadził jawny, ogólnokrajowy rejestr zbiorów danych osobowych przez 20 lat. Zadaniu temu odpowiadał

m.in. nałożony na administratorów obowiązek zgłaszania do rejestracji zbiorów danych osobowych, zgłaszania zmian w prowadzonych zbiorach oraz zawiadamianie o zaprzestaniu przetwarzania danych w zbiorze. ***Przez ten czas wnioskodawcy zgłosili do rejestracji 304 398 zbiorów danych osobowych.*** *Natomiast 25 maja 2018 r., w związku z rozpoczęciem stosowania ogólnego rozporządzenia o ochronie danych, wygasł obowiązek zgłaszania do rejestracji zbiorów danych osobowych. Nadszedł zatem czas na podsumowanie 20 lat rejestracji zbiorów danych osobowych.*

Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych przewidywała obowiązek zgłoszenia zbioru danych do rejestracji w art. 40 – przepis ten wszedł w życie 30 kwietnia 1998 r. Obowiązek ten był zasadą, od której były przewidziane wyjątki – wymienione w art. 43 ust. 1 i 1 a tej ustawy. Wykonanie obowiązku zgłoszenia zbioru danych do rejestracji polegało na złożeniu przez administratora wypełnionego formularza zgłoszenia zawierającego określone prawem informacje opisujące proces przetwarzania danych osobowych w konkretnym zbiorze.

Administrator informował w ten sposób m.in. o tym, jakie dane zamierza przetwarzać, jakich osób będą one dotyczyć, w jakim celu dane będą przetwarzane, wskazywał, jaka jest podstawa prawna planowanych przez niego działań oraz jaki zastosował poziom środków bezpieczeństwa. Przez przeważający okres minionych 20 lat liczba wpływających zgłoszeń do rejestracji zbiorów danych rosła w tempie lawinowym, **np. 2004 r. – 2 787, 2008 r. – 5 776, 2012 r. – 21 580, a w 2014 r. – 43 300** zgłoszeń. Wiele z tych zgłoszeń pochodziło od podmiotów publicznych, przetwarzających dane w związku z realizacją swoich ustawowych zadań.

Z każdym rokiem rosła liczba zgłoszeń zbiorów składanych przez podmioty z sektora prywatnego – przedsiębiorców, którzy zgłaszali zamiar przetwarzania danych przy pomocy nowoczesnych urządzeń i rozwiązań technologicznych, takich jak np. przetwarzanie danych w aplikacjach mobilnych, świadczenie usług z wykorzystaniem danych geolokalizacyjnych, czy stosowanie tzw. technologii ubieralnych.

Najważniejszym celem rejestracji zbiorów było sprawowanie przez GIODO nadzoru nad przestrzeganiem przepisów ustawy o ochronie danych osobowych poprzez prowadzenie wstępnej kontroli w zakresie prawidłowości przetwarzania danych osobowych. GIODO, na podstawie przekazanych w treści zgłoszenia informacji, badał, czy administrator przestrzega m.in. zasad przetwarzania danych określonych w art. 23–28 ustawy, np. zasady adekwatności.

Dużą zaletą przyjęcia takiego rozwiązania była zatem możliwość eliminowania nieprawidłowości na etapie postępowania rejestracyjnego, zanim dojdzie do pozyskania pierwszych danych do zbioru.

Jeżeli planowane przez administratora działania były zgodne z przepisami ustawy, zbiór danych był wpisywany do jawnego, ogólnokrajowego rejestru zbiorów danych osobowych. Natomiast w przypadku naruszenia przepisów, GIODO odmawiał rejestracji zbioru w drodze decyzji administracyjnej, a zatem władczo rozstrzygał o legalności przetwarzania danych przez administratora. Najczęściej decyzje te nakazywały usunięcie danych nieadekwatnych do celu przetwarzania lub wprowadzenie dodatkowych środków zabezpieczających dane zgromadzone w zbiorze na odpowiednim poziomie.

W przypadku wydania decyzji o odmowie rejestracji zbioru administrator, zgodnie z art. 44 ust. 4 ustawy, mógł zgłosić ponownie zbiór danych do rejestracji po usunięciu wad, które były powodem odmowy jego rejestracji. Jedynie w **45** przypadkach administratorzy zwrócili się do Generalnego Inspektora z **wnioskami o ponowne rozpatrzenie sprawy**.

Do 25 maja 2018 r. do rejestru zostało wpisanych 187 800 zbiorów. GIODO wydał 2 300 decyzji o odmowie rejestracji zbioru danych. Jednak nie każde postępowanie rejestracyjne kończyło się wpisaniem zbiorem do rejestru lub wydaniem decyzji o odmowie rejestracji.

W przypadku zgłoszenia zbioru niepodlegającego obowiązkowi rejestracyjnemu lub jeżeli zgłoszenia dokonał podmiot niebędący administratorem, lub którego zgłoszenie nie dotyczyło wyłącznie jednego zbioru danych, GIODO zawiadamiał pisemnie wnioskodawcę o powodach i podstawie prawnej niedokonania wpisu w rejestrze. Korespondencja z wnioskodawcami posiadała

także istotny walor edukacyjny, zawierała m.in. informacje i omówienie zasad przetwarzania danych, pomocne przy ocenie stanu faktycznego związanego z przetwarzaniem. W czasie istnienia obowiązku rejestracyjnego Generalny Inspektor wysłał:

- prawie **8 000 pism informujących o braku obowiązku zgłoszenia do rejestracji zbioru** (wynikającym z przesłanek określonych w art. 43 ust. 1 i 1a ustawy).
- ponad **13 500 informacji o braku podstaw do dokonania wpisów w rejestrze z innych przyczyn** (zgłoszenia złożyły podmioty nie będące administratorami danych lub zgłoszenia obejmowały więcej niż jeden zbiór danych osobowych).

Realizując zadanie informowania o zarejestrowanych zbiorach, GIODO wydał w ciągu 20 lat administratorom, z urzędu lub na wniosek, ponad **52200 zaświadczeń o zarejestrowaniu zbioru danych**.

Ponadto organ do spraw ochrony danych osobowych, w celu zapewnienia aktualności rejestru, wydał **2 687 decyzji o wykreśleniu zbioru** danych z rejestru, w przypadku zaprzestania przetwarzania danych osobowych w zarejestrowanym zbiorze.

W ciągu 20 lat istnienia obowiązku rejestracyjnego, dwukrotnie, w maju 2004 r. oraz grudniu 2008 r., zmianie ulegał wzór formularza zgłoszenia zbioru danych do rejestracji. Ówczesny Departament Rejestracji Zbiorów Danych Osobowych, opracowując nowy wzór formularza, wprowadzał możliwe uproszczenia formularza, dążąc do ułatwienia administratorom spełnienia obowiązku rejestracyjnego. Potrzeba wprowadzenia zmian w tym zakresie wynikała z faktu, że poprawne wypełnienie wcześniej obowiązującego formularza zgłoszenia często sprawiało administratorom trudności (pojawiały się one szczególnie w części D zgłoszenia, dotyczącej sposobu zbierania i udostępniania danych oraz części E zawierającej informacje o środkach technicznych i organizacyjnych zastosowanych w celu zabezpieczenia danych).

Bardzo istotnym narzędziem, przyjaznym administratorom, był wdrożony w 2006 r. w Biurze Generalnego Inspektora Ochrony Danych Osobowych system informatyczny o nazwie „Platforma elektronicznej platforma komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych (e-GIODO)”[203]. Realizacja projektu systemu e-GIODO stała się możliwa dzięki współfinansowaniu ze środków Europejskiego Funduszu Rozwoju Regionalnego. W 2007 r., tj. w pierwszym pełnym roku funkcjonowania programu wspomagającego elektroniczne wypełnienie zgłoszenia, proporcje wpływu zgłoszeń wypełnionych metodą tradycyjną (bez użycia komputera) do zgłoszeń wypełnionych w sposób elektroniczny wyniosły odpowiednio 75 do 25 proc. Rosnąca wśród wnioskodawców z roku na rok popularność udostępnionego narzędzia, wynikająca m.in. z postępującej informatyzacji zarówno przedsiębiorców, jak i podmiotów publicznych, sprawiła, że przedstawiona proporcja uległa odwróceniu o 180 stopni w ciągu zaledwie 4 lat i z niewielkimi wahaniami trwała do końca 2017 r.

Program wspomagający wypełnienie zgłoszenia do rejestracji zbioru zawierał na każdym etapie przygotowywania wniosku system podpowiedzi i komunikatów o błędach popełnionych przez wnioskodawcę. Funkcjonalność ta eliminowała możliwość popełnienia częstych błędów w procesie wypełniania formularza, w szczególności w zakresie sposobu spełniania wymagań technicznych i organizacyjnych zastosowanych w celu zabezpieczenia zbioru danych osobowych (części E i F zgłoszenia). W rezultacie możliwe było szybsze zakończenie większej liczby postępowań rejestracyjnych, bez konieczności prowadzenia postępowania wyjaśniającego. Wdrożenie systemu e-GIODO umożliwiało ponadto przeglądanie Rejestru Zbiorów Danych Osobowych za pośrednictwem Internetu i wyszukiwanie zarejestrowanych zbiorów danych za pomocą kilku kryteriów, m.in. nazwy zbioru, nazwy administratora, czy jego siedziby lub numeru REGON.

Obowiązek zgłaszania zbiorów do rejestracji GIODO przeszedł do historii z dniem 25 maja 2018 r. RODO znosi ogólny obowiązek zgłaszania do rejestracji operacji przetwarzania danych i kontroli wstępnej sprawowanej przez GIODO, kładąc nacisk na samokontrolę administratora począwszy

[203] https://archiwum.giodo.gov.pl/1520040

od etapu projektowania zamierzonego przetwarzania i konsultacje z organem nadzorczym w tych przypadkach, które szczególnie zagrażają prywatności osób. W praktyce oznacza to, że przed rozpoczęciem przetwarzania to administrator, a nie jak dotychczas organ nadzorczy w ramach kontroli wstępnej, będzie zobowiązany ocenić planowane operacje przez pryzmat poszanowania praw osób, których dane dotyczą. Organ natomiast skonsultuje, na wniosek administratora, zastosowane środki ochrony i zaleci, w razie potrzeby, dalsze działania. Rezygnacja z ogólnego obowiązku informowania organu o operacjach przetwarzania danych osobowych na rzecz skoncentrowania się na działaniach szczególnie niebezpiecznych oraz podkreślenie obowiązku dokonania przez administratorów szczegółowej oceny stanu faktycznego, zdiagnozowania zagrożeń i podjęcia przez nich adekwatnych środków zaradczych jest obecnie niezbędna w świetle wyzwań stawianych m.in. przez rozwój informatyzacji, który daje możliwość przetwarzania danych osobowych stwarzającego zagrożenia nieznane w dobie uchwalania i implementacji do polskiego prawa dyrektywy 95/46 WE.

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA

Zgodnie z treścią art. 57 RODO, podstawowe zadania organu nadzorczego obejmują m.in.:

- *upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumieniem tych zjawisk, ze szczególnym uwzględnieniem działań skierowanych do dzieci[204];*
- *upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO[205];*
- *udzielanie osobom, której dane dotyczą, na ich żądanie informacji o wykonywaniu praw przysługujących im na mocy RODO , a w stosownym przypadku współpracę w tym celu z organami nadzorczymi innych państw członkowskich[206].*

Organ właściwy w sprawie ochrony danych osobowych podejmuje szereg działań edukacyjno-informacyjnych, których celem jest zwiększanie świadomości społeczeństwa w zakresie prawa do prywatności i ochrony danych osobowych oraz podnoszenie poziomu wiedzy na temat ochrony danych osobowych w Polsce.

1. Działalność edukacyjna

1.1. Szkolenia

Szkolenia podmiotów zewnętrznych i warsztaty konsultacyjne
W ramach prowadzonej działalności edukacyjnej w 2018 r., organ ds. 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.

[204] Art. 57.1.b RODO
[205] Art. 57.1.d RODO
[206] Art. 57.1.e RODO

Szkolenia przeprowadzane przez przedstawicieli organu nadzorczego dla kadry zarządzającej oraz pracowników różnych instytucji i organizacji dotyczyły stosowania nowych przepisów o ochronie danych osobowych przez organy administracji publicznej i inne podmioty.

W sumie w 2018 r. przeprowadzono **51 szkoleń podmiotów zewnętrznych** (*vide* załącznik 2).

Wśród podmiotów, które w 2018 r. zwróciły się do organu nadzorczego z prośbą o przeprowadzenie szkolenia znalazły się: Krajowa Szkoła Administracji Publicznej, Warszawski Uniwersytet Medyczny, Wojewódzki Urząd Pracy w Kielcach, Wojewódzki Urząd Pracy w Gdańsku oraz agencje zatrudnienia z województwa pomorskiego, Urząd Marszałkowski Województwa Małopolskiego, urzędy województwa podlaskiego, dolnośląskiego i świętokrzyskiego, Ministerstwo Rodziny, Pracy i Polityki Społecznej, Ministerstwo Spraw Wewnętrznych i Administracji i Ministerstwo Finansów, a także NSZZ „Solidarność" oraz Konferencja Wyższych Przełożonych Zakonów Męskich w Polsce. Przedstawiciele organu nadzorczego przeprowadzili także szkolenia dla sędziów Wojewódzkiego Sądu Administracyjnego w Warszawie, pracowników Kancelarii Sejmu RP, Kancelarii Prezesa Rady Ministrów w ramach VI Dnia Otwartego dla służby cywilnej oraz szkolenie dla przedstawicieli MŚP z Dolnego Śląska.

Prezes UODO przeprowadził szkolenie realizowane w ramach IX edycji ogólnopolskiego odbywającego się cyklicznie programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli" (15–16.10.2018) oraz wykład online **„Inspektor ochrony danych – fachowy doradca i audytor obowiązkowy w każdej szkole"**, przygotowany dla uczestników programu.

Podczas konferencji, szkoleń czy spotkań organizowanych przez organ nadzorczy lub współpracujące z nim podmioty, eksperci (pracownicy organu) udzielali **indywidualnych nieodpłatnych porad prawnych** dla zainteresowanych osób, w tym przedstawicieli mediów. Inicjatywa konsultacji prawnych była odpowiedzią na sygnalizowaną potrzebę dotarcia do szerszego odbiorcy z informacjami z zakresu prawa do prywatności i ochrony danych osobowych i spotkała się z uznaniem opinii publicznej.

Na uwagę zasługują także spotkania w formule szkolenia w związku z przygotowaniami do tworzenia **kodeksów postępowania w świetle RODO** przez podmioty sektorów m.in.: medycznego, marketingowego, informatycznego czy banków i innych instytucji finansowych. Pierwsze z warsztatów odbyły się w minionym roku sprawozdawczym (2017) na Warszawskim Uniwersytecie Medycznym oraz Śląskim Uniwersytecie Medycznym w Katowicach w związku z pracami nad projektem kodeksu postępowania z zakresu ochrony danych osobowych dla uczelni medycznych. W analizowanym 2018 r. organ nadzorczy kontynuował szkolenie podmiotów przygotowujących kodeksy postępowania w świetle RODO, organizując warsztat poświęcony temu tematowi (11.01.2018). W ramach warsztatu odbyły się prezentacje podmiotów pracujących nad kodeksem postępowania w swojej organizacji oraz przedstawiono główne założenia, treść i procedurę zatwierdzania kodeksów.

Szkolenia sektorowe ABI/IOD

W 2018 r. organ do spraw ochrony danych kontynuował – zainicjowany w 2016 r. – cykl nieodpłatnych szkoleń dla administratorów bezpieczeństwa informacji (ABI)/inspektorów ochrony danych (IOD) wybranych sektorów.

Od 2016 r. odbyło się 12 ww. szkoleń, z czego pięć w 2018 r. **Trzy szkolenia dedykowane były administratorom bezpieczeństwa informacji (ABI)** sektora szkolnictwa (27.02.2018)[207] i przedszkoli (24.04.2018)[208] a **jedno szkolenie inspektorom ochrony danych (IOD)** sektora mieszkalnictwa (26.06.2018)[209]Celem ostatniego z wymienionych było omówienie obowiązków administratorów

[207] https://uodo.gov.pl/pl/189/455
[208] https://uodo.gov.pl/pl/189/457
[209] https://uodo.gov.pl/pl/189/366

wynikających z RODO oraz nowej ustawy o ochronie danych osobowych, z uwzględnieniem specyfiki przetwarzania danych osobowych w tym sektorze, a także przedstawienie roli IOD.

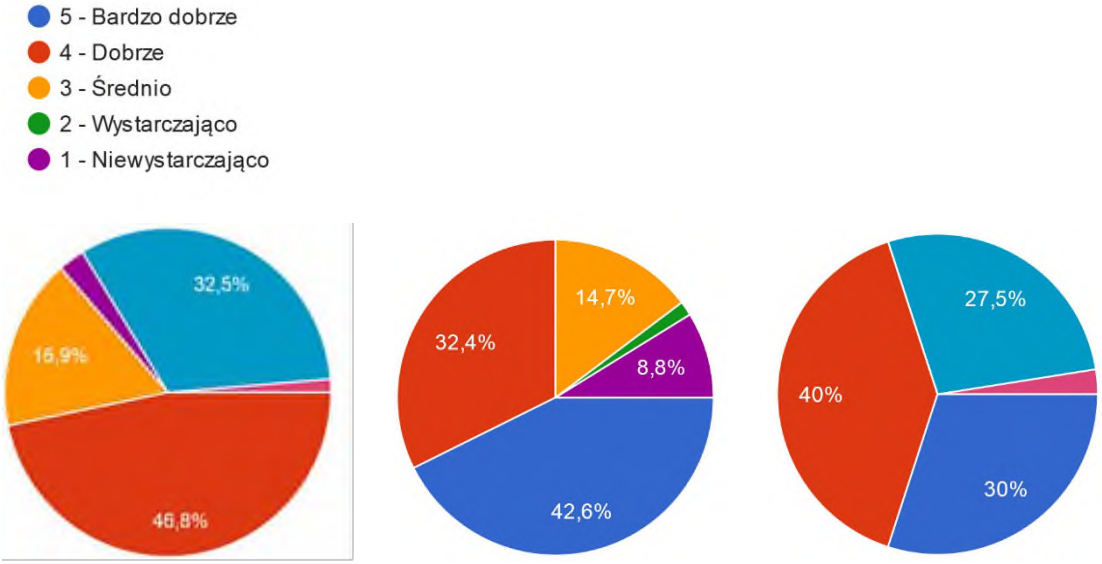
Kolejne dwa szkolenia dla inspektorów ochrony danych (IOD) „Obowiązki pracodawców w zakresie przetwarzania danych osobowych" (4.10.2018) i "Ocena skutków dla ochrony danych osobowych" (19.12.2018), odbywały się już w zmienionej formule. Szkolenie przeprowadzone 4.10.2018 r. przez ekspertów UODO adresowane było do IOD wszystkich sektorów i dotyczyło zagadnień istotnych dla **sektora zatrudnienia**. Wśród tematów znalazły się te, które budziły największe wątpliwości, tj. np. jak zawierać umowy powierzenia przetwarzania danych, właściwie prowadzić rekrutację pracowników, czy monitoring w miejscu pracy. **Szkolenie dla IOD zorganizowane 19 grudnia 2018 r.** dotyczyło **oceny skutków dla ochrony danych, jako realizacji** wskazanej w przepisach RODO zasady rozliczalności.

Łącznie w szkoleniach zorganizowanych dla ABI/IOD wzięło udział ponad 1000 uczestników. Szkolenia zorganizowane przez UODO w nowej formule transmitowane były na żywo, a następnie zostały udostępnione na kanale YouTube UODO, osiągając do tej pory już ponad 30 tysięcy wyświetleń *(dane z czerwca 2019).*

Sektorowe szkolenia koncentrowały się na nowych unijnych przepisach o ochronie danych osobowych oraz przepisach krajowych, mających zastosowanie do przetwarzania danych w określonej dziedzinie działalności. Szkolenie nie tylko do podniosły poziom wiedzy ABI / IOD, obsługujących daną branżę, ale stanowiły także okazję do wymiany doświadczeń, rozwiązań i dobrych praktyk pomiędzy uczestnikami.

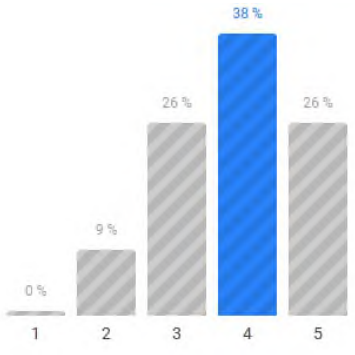
Po przeprowadzonych szkoleniach w II półroczu 2018 r. do ich uczestników wysłana była ankieta ewaluacyjna z prośbą o ocenę.

W odniesieniu do szkoleń dla ABI sektora szkolnictwa, przedszkoli i mieszkalnictwa, poziom satysfakcji respondentów przedstawiał się następująco:

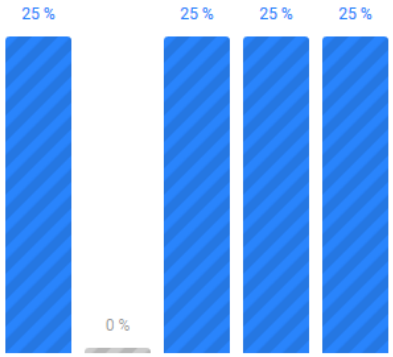


Poziom satysfakcji respondentów w skali od 1 do 5 w odniesieniu do szkoleń dla IOD przedstawiał się następująco:

Ocena w skali od 1 do 5



Ocena szkolenia pt. „Obowiązki pracodawców w zakresie przetwarzania danych osobowych" (4.10.2018 r.) w skali od 1 do 5.



Ocena szkolenia pt. „Ocena skutków dla ochrony danych osobowych" (19.12.2018 r.) w skali od 1 do 5.

Szkolenia dla organizacji pozarządowych i jednostek samorządu terytorialnego (jst)

W analizowanym okresie **sprawozdawczym przedstawiciele organu nadzorczego prowadzili szkolenia dla organizacji pozarządowych oraz jednostek samorządu terytorialnego.**

Szkolenia dla przedstawicieli organizacji pozarządowych współorganizowane były we współpracy z Narodowym Instytutem Wolności (NIW). Celem szkoleń było wyjaśnienie, jak w praktyce podmioty tego sektora mają chronić dane osobowe swoich pracowników, współpracowników, w tym zwłaszcza wolontariuszy, jakich zasad trzeba przestrzegać, wykorzystując dane osobowe dzieci i młodzieży itp. Przybliżeniu tych zasad służyła prowadzona nieprzerwanie kampania edukacyjno-informacyjna „Gotowi na RODO" prowadzona przez organ nadzorczy we współpracy z Narodowym Instytutem Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego (NIW – CRSO) w formule szkoleń we wszystkich miastach wojewódzkich w Polsce. Na potrzeby wyżej wspomnianej kampanii przygotowano bezpłatny **podręcznik dla organizacji pozarządowych,** pomocny w praktycznym stosowaniu nowego prawa o ochronie danych osobowych. W szkoleniach przeprowadzonych w okresie od kwietnia do października 2018 r., uczestniczyło 1 470 osób z prawie 1000 różnych organizacji pozarządowych.

Szkolenia dla przedstawicieli jednostek samorządu terytorialnego (jst) zorganizowano we współpracy z Narodowym Instytutem Samorządu Terytorialnego (NIST).

Adresatem tych szkoleń byli pracownicy odpowiedzialni za bezpieczeństwo danych osobowych w jednostkach samorządu terytorialnego. **Szkolenia jst** odbywały się w 12 miastach wojewódzkich w okresie od czerwca 2018 r. do marca 2019. Łącznie w szkoleniach wzięło w nich udział 1084 uczestników z 554 jednostek samorządu terytorialnego (starostw powiatowych, urzędów marszałkowskich, miast i gmin).

Szkolenia dla przedstawicieli jednostek samorządu terytorialnego i organizacji pozarządowych w ramach współpracy z NIST i NIW dotyczące zmian w zakresie ochrony danych osobowych w świetle RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, organizowane były we wszystkich 16 województwach na terenie kraju. W roku sprawozdawczym odbyło się 19 takich szkoleń z udziałem ok. 2 500 tys. osób.

Konkursy

W analizowanym 2018 r. organ nadzorczy był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

1. Konkurs na esej dotyczący zagadnień z zakresu ochrony danych osobowych

Organ ds. ochrony danych osobowych był organizatorem VIII edycji konkursu dla studentów prawa i administracji na esej dotyczący zagadnień z zakresu ochrony danych osobowych. Organizowany cyklicznie konkurs ma 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.

„Pozyskiwanie danych osobowych dla celów prowadzenia portalu studenckiego" to tytuł edycji konkursu zorganizowanego w 2018 r. przez Biuro GIODO, przy wsparciu merytorycznym Kobylańska & Lewoszewski Kancelaria Prawna sp.j. Przedmiotem konkursu było przygotowanie eseju na temat prawidłowości zbierania zgód od studentów korzystających z portalu internetowego do wymiany notatek między studentami oraz kwestia ważności pozyskanych zgód w świetle przepisów ogólnego rozporządzenia o ochronie danych.

Konkurs skierowany był do studentów prawa i administracji III–V roku studiów jednolitych i I–III roku studiów drugiego stopnia. Laureaci konkursu otrzymali nagrody rzeczowe oraz nagrody specjalne w postaci nieodpłatnych praktyk w organie nadzorczym.

2. „Złote Pióro" – konkurs dla szkół i ośrodków doskonalenia nauczycieli w ramach programu „Twoje dane – Twoja sprawa"

Organ nadzorczy zorganizował VIII edycję konkursu dla szkół i ośrodków doskonalenia nauczycieli w ramach ogólnopolskiego programu edukacyjnego *„Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli"* , którego zadaniem jest promowanie najciekawszych inicjatyw mających na celu upowszechnianie wśród uczniów i nauczycieli wiedzy o ochronie danych osobowych i prawa do prywatności. Przedmiotem oceny w ramach konkursu były działania podjęte przez uczestników programu oraz partnerów metodycznych podczas VIII edycji programu, które wyróżniały się pomysłowością i wysokim poziomem merytorycznym przygotowanych materiałów, szerokim zasięgiem i efektywnością oddziaływania.

Główną nagrodą – Złotym Piórem – uhonorowany został projekt o nazwie „Odkoduj Swoje Dane" opracowany i realizowany przez XI Liceum Ogólnokształcące im. Marii Dąbrowskiej w Krakowie. W pracy tej opisano VI etapów działań skierowanych do uczniów klas pierwszych i drugich liceum. Działania te obejmowały: cykl zajęć edukacyjnych na temat ochrony danych osobowych i prawa do prywatności opracowanych przy wykorzystaniu otrzymanych scenariuszy oraz materiałów zamieszczonych na stronie internetowej GIODO/UODO, stworzenie przez ucznia fanpage'a dotyczącego ochrony danych osobowych i bezpieczeństwa cyfrowego, studium przypadku – omówienie sytuacji problemowych i zastosowanie wiedzy w praktyce, opracowanie autorskiego scenariusza zajęć i przeprowadzenie lekcji języka polskiego w oparciu o fake newsy, przygotowanie przez uczniów narzędzi do sprawdzenia wiedzy (krzyżówki, konkurs na rebus, film nakręcony przez uczniów), testowanie narzędzi weryfikacji wiedzy i ulotek informacyjnych na podstawie zdobytej wiedzy, upowszechnienie materiałów w środowisku lokalnym (rodzice, sąsiedzkie przedszkole, współpraca z gimnazjum), organizacja „Cyfrowo bezpiecznej gry miejskiej" dla uczniów. Zaangażowanie szkoły w realizację programu „Twoje dane – Twoja sprawa" i niezwykle ciekawe zajęcia praktyczne stanowią przykład najlepszych praktyk w zakresie edukacji uczniów szkoły

ponadpodstawowej nt. ochrony danych osobowych, którzy w ramach realizowanych działań zdobywają doświadczenie i praktyczną wiedzę z zakresu ochrony danych osobowych.

Kolejni zwycięzcy to szkoła podstawowa z Łodzi nagrodzona za projekt lekcji koleżeńskiej dla nauczycieli „ESCAPE ROOM – ODOland" i technikum z Warszawy za inicjatywę pod nazwą „W świecie DANYCH OSOBOWYCH – dane w podchodach zebrane(?)", którzy zajęli II miejsce *ex aequo.*

III miejsce zajęła Gminna Szkoła Podstawowa im. Polskich Noblistów w Oławie za organizację gry z okazji Międzynarodowego Dnia Nowych Technologii „Mój Świat – cyfrowy świat".

Z uwagi na walory edukacyjne nadesłanych prac, dodatkowo wyróżnione zostały prace trzech szkół:

- Publicznej Szkoły Podstawowej nr 4 im. Kornela Makuszyńskiego z oddziałami przedszkolnymi w Strzegomiu za szkolenie/kampanię edukacyjną „Bezpieczny senior";
- Szkoły Podstawowej nr 11 im. Henryka Sienkiewicza w Piotrkowie Trybunalskim za inicjatywę „Dzielenie się wiedzą ze społecznością szkolną i środowiskiem lokalnym";
- IX Liceum Ogólnokształcącego im. Juliusza Słowackiego z Oddziałami Sportowymi w Radomiu i Publicznej Szkoły Podstawowej nr 17 im. Przyjaciół Dzieci z włączonym Publicznym Gimnazjum nr 3 im. Jana Kochanowskiego w Radomiu za organizację konkursu.

Uroczyste wręczenie nagród i wyróżnień w konkursie odbyło się podczas spotkania podsumowującego VIII edycję programu **8 czerwca 2018 r. w** Warszawie, podczas którego laureaci zaprezentowali swoje prace konkursowe.

3. Konkurs dla uczniów – w ramach VIII edycji programu „Twoje dane – Twoja sprawa"

Celem konkursu było upowszechnienie wiedzy na temat prawa do prywatności i ochrony danych osobowych poprzez przygotowanie **infografiki, mini-poradnika lub filmu pt. „Mój pierwszy telefon – ochrona prywatności w sieci".**

W swoich pracach uczniowie – uczestnicy VIII edycji programu „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli.", podkreślili istotne aspekty ochrony prywatności, takie jak m.in.: mocne hasła dostępu do kont, fizyczne

zabezpieczenie smartfona, wylogowywanie się z portali społecznościowych, instalowanie antywirusów i aktualizacja oprogramowania, ściąganie aplikacji tylko ze znanych źródeł, stosowanie zasady ograniczonego zaufania przy udostępnianiu danych w sieci i nawiązywaniu znajomości, poszanowanie prywatności osób bliskich i ochronę ich wizerunku, udostępnianie danych za zgodą osoby, której dane dotyczą.

Z uwagi na wysoki poziom merytoryczny przysłanych prac komisja konkursowa złożona z przedstawicieli organu nadzorczego oraz Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie wybrała trzy najlepsze prace oraz wyróżniła jedenaście. I miejsce zajął uczeń Szkoły Podstawowej nr 1 w Sochaczewie, II miejsce – uczniowie Zespołu Szkół Ponadgimnazjalnych nr 2 w Krotoszynie, zaś III – uczniowie Szkoły Podstawowej nr 11 im. H. Sienkiewicza w Piotrkowie Trybunalskim.

Nagrody i wyróżnienia zostały wręczone podczas spotkania podsumowującego VIII edycję programu edukacyjnego 8 czerwca 2018 r.

Projekty i programy

W roku sprawozdawczym 2018, organ nadzorczy kontynuował udział w projektach rozpoczętych we wcześniejszych latach, m.in. w projekcie „**e-OpenSpace – Europejska innowacyjna otwarta platforma na rzecz elektronicznego utrzymywania współpracy i zrównoważonego zapewniania kształcenia zorientowanego na dorosłych w zakresie ochrony prywatności i danych osobowych.**”, którego realizacja rozpoczęła się we wrześniu 2017 r. , a jego zakończenie planowane jest na sierpień 2019 r. Projekt ten finansowany jest w ramach programu Erasmus+ „Akcja 2 – Współpraca na rzecz innowacji i wymiany dobrych praktyk, Działanie – Partnerstwo strategiczne na rzecz edukacji osób dorosłych”. Koordynatorem projektu jest Komisja Ochrony Danych Osobowych w Bułgarii (CPDP), a partnerami: GIODO/UODO, Chorwacka Agencja Ochrony Danych Osobowych (AZOP), Uniwersytet Sofijski im. św. Klemensa z Ochrydy, Uniwersytet Jagielloński oraz Włoska organizacja pozarządowa (GVMAS ONLUS).

Celem projektu e-OpenSpace jest stworzenie elektronicznej przestrzeni – platformy złożonej z dwóch części: publicznej i prywatnej. Platforma ma za zadanie ułatwić obywatelom dostosowanie się do nowego systemu prawnego dotyczącego ochrony danych osobowych.

Poprzez prywatną część platformy możliwa będzie komunikacja pomiędzy organami ochrony danych osobowych. Komunikacja ta odbywać się będzie poprzez wymianę dokumentów oraz innych informacji niezbędnych do współpracy oraz realizacji nowego prawa o ochronie danych osobowych w zakresie obowiązku edukacyjnego organów ochrony danych osobowych. Platforma ułatwi organom ochrony danych wymianę informacji i tym samym zapewni danym bezpieczeństwo.

Publiczna część platformy, przeznaczona przede wszystkim dla praktyków oraz wszystkich zainteresowanych, umożliwi nieformalną edukację w zakresie nowego prawa o ochronie danych osobowych i prywatności. Materiały będą dostępne po utworzeniu przez użytkownika konta. Platforma zostanie zbudowana w specjalnie dla niej wydzielonym miejscu na serwerze każdego z trzech urzędów ochrony danych osobowych i będzie dostępna poprzez oficjalną stronę internetową urzędów.

W skład materiałów edukacyjnych nowo powstałej platformy (w języku, angielskim, polskim, chorwackim, bułgarskim i włoskim) będą wchodziły m.in.: nagrania prezentacji, dokumenty, sekcja pytań i odpowiedzi.

Organ nadzorczy w styczniu 2018 roku rozpoczął także realizację nowych przedsięwzięć, wśród których wymienić należy międzynarodowy projekt **„T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych”**. Celem projektu jest wsparcie organów nadzorczych oraz inspektorów ochrony danych z podmiotów publicznych, na rzecz szkoleń w zakresie nowego prawa o ochronie danych osobowych. Projekt ma pomóc w wypracowaniu jednolitego rozumienia i interpretacji wymogów RODO, a w konsekwencji wzmocnić wzajemne zaufanie między organami ochrony danych w zakresie stosowania nowego prawa o ochronie danych osobowych.

Biuro GIODO rozpoczęło realizację projektu T4DATA w styczniu 2018 r., w ramach którego wspólnie z organami ochrony danych z Włoch, Hiszpanii, Bułgarii i Chorwacji przygotowany został cykl szkoleń dla ABI (obecnie IOD) z sektora publicznego. Projekt zakłada przeszkolenie wybranych pracowników organów nadzorczych, którzy przeprowadzą cztery szkolenia dla administracji publicznej w swoim kraju. W Polsce szkolenia dla administracji publicznej obejmą 600 osób. Dodatkowo uruchomiona zostanie platforma, na której możliwe będzie skorzystanie z oferty webinariów poświęconych właściwemu wdrożeniu RODO w podmiotach z sektora publicznego. Projekt potrwa dwa lata.

Projekt współfinansowany jest przez Komisję Europejską w ramach Programu „Prawa, równość i obywatelstwo na lata 2014–2020".

W 2018 roku kontynuowano realizację ogólnopolskiego programu edukacyjnego dla szkół **„Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli",** organizowanego nieprzerwanie od 2009 r. pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.**".** W roku sprawozdawczym zakończyła się VIII edycja tego programu realizowana w roku szkolnym 2017/2018 oraz rozpoczęła się IX edycja (rok szkolny 2018/2019).

Organizatorem programu „Twoje dane – Twoja sprawa", jest Biuro GIODO/Prezes UODO, zaś partnerami: Gliwicki Ośrodek Metodyczny oraz Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

Głównym celem programu jest poszerzenie oferty edukacyjnej placówek doskonalenia zawodowego nauczycieli oraz szkół o treści związane z ochroną danych osobowych i prawem każdego człowieka do prywatności.

Jednym z etapów programu jest przeszkolenie i wyposażenie kadry pedagogicznej szkół i placówek doskonalenia nauczycieli w materiały edukacyjne zawierające m.in. informacje dotyczące zasad ochrony danych osobowych i scenariusze lekcji, jak również przygotowanie nauczycieli do zadania, jakim jest kształtowania świadomych, odpowiedzialnych i otwartych postaw wśród uczniów. Placówki zgłoszone do programu otrzymały materiały edukacyjne podczas dwudniowego obowiązkowego szkolenia, które dla VIII edycji TDTS odbyło się 26–27 października 2017 r., zaś dla IX edycji – 15–16 października 2018 r.

W VIII edycji TDTS 2017/2018 program realizowały 334 placówki – ośrodki doskonalenia zawodowego nauczycieli, szkoły podstawowe, gimnazja, szkoły ponadpodstawowe i ponadgimnazjalne – w tym 262 placówki, które przystąpiły do programu po raz pierwszy. W VIII edycji Programu uczestniczyło ponad 50 tys. uczniów polskich szkół[210].

[210] Dane obliczone na podstawie raportów końcowych z realizacji inicjatywy, przesłanych przez 143 placówki.

Przeszkolonych zostało 226 koordynatorów, którzy w poszczególnych szkołach i ośrodkach zorganizowali spotkania szkoleniowe rad pedagogicznych i spotkania dyrektorów szkół. W szkoleniu udział wzięło 1 471 nauczycieli, którzy następnie wprowadzali treści związane z ochroną danych osobowych i prawem do prywatności na lekcje wychowawcze oraz lekcje przedmiotów ogólnokształcących. W ramach realizacji programu, nauczyciele angażowali w działania społeczność szkolną i środowisko lokalne po to, aby idea ochrony prywatności i danych osobowych mogła być stałym elementem edukacji szkolnej i pozaszkolnej.

W 4 945 lekcjach i wydarzeniach tematycznych w całej Polsce uczestniczyło 50 743 uczniów. Zrealizowano ponad 900 działań edukacyjnych, a w tym 346 z okazji Dnia Ochrony Danych Osobowych.

Program TDTS cieszy się niesłabnącym zainteresowaniem wśród placówek oświatowych, czego dowodem jest rozpoczęcie kolejnej **jego edycji w roku szkolnym 2018/2019.**

IX edycja zainaugurowana została wspomnianym wcześniej szkoleniem dla koordynatorów, zorganizowanym przez Prezesa UODO. Uczestnicy szkolenia otrzymali przygotowany przez UODO pakiet materiałów edukacyjnych, zawierający broszury informacyjne dotyczące przetwarzania danych osobowych, scenariusze lekcji, prezentacje multimedialne i inne pomoce dydaktyczne ułatwiające realizację programu. Program ten był realizowany poprzez zajęcia lekcyjne i pozalekcyjne oraz organizację wydarzeń tematycznych.

Uczniowie szkół biorących udział w programie mieli okazję wykazać się swoimi pomysłami, umiejętnościami i talentami (plastycznymi, aktorskimi i sportowymi). Przy okazji dobrej zabawy i aktywnie spędzonego czasu, zdobywali wiedzę i umiejętności praktyczne w zakresie skutecznej ochrony danych osobowych zarówno własnych, jak i swoich bliskich. Uczestniczyli w konkursach, zabawach, warsztatach, spotkaniach z ekspertami oraz w zajęciach terenowych.

N**auczyciele uczestniczący w programie**, poprzez udział w specjalistycznych szkoleniach, przy wsparciu ekspertów UODO, otrzymanych podczas organizowanych seminariów i webinariów materiałach edukacyjnych, zdobywali wiedzę na temat ochrony danych osobowych w szkołach oraz obowiązków wynikających z RODO w sektorze oświaty. Wieloletnie doświadczenie organu nadzorczego przy realizacji programu pokazało, że w łatwy i przystępny sposób można skutecznie uczyć dzieci i młodzież bezpiecznego poruszania się w świecie nowoczesnych technologii, a także, że ochrona prywatności powinna być nieodłącznym elementem edukacji cyfrowej.

Cennym wsparciem dla nauczycieli i pracowników placówek oświatowych w wykonywaniu ich codziennych obowiązków był poradnik Prezesa UODO dla szkół „Ochrona danych osobowych w szkołach i placówkach oświatowych".

Do IX edycji programu przystąpiło 334 placówek oświatowych.

Wszystkie lekcje i wydarzenia, które odbywały się w ramach programu były realizowane w celu upowszechnienia wiedzy o ochronie danych osobowych, promowania wśród dzieci i młodzieży zasad ochrony danych osobowych, rozwijania wiedzy i umiejętności w zakresie bezpiecznego funkcjonowania w dobie szybkiego rozwoju nowych technologii, kształtowania świadomych i odpowiedzialnych postaw wśród uczniów, jak również w celu zwrócenia uwagi środowiska lokalnego, a przede wszystkim rodziców i nauczycieli na istotę ochrony danych osobowych i prawa do prywatności uczniów. Mając na uwadze wymienione cele programu, będzie on kontynuowany w kolejnych latach, aby sprostać rosnącemu zapotrzebowaniu na tego rodzaju wiedzę w placówkach oświatowych.

Warto również podkreślić, że z roku na rok, uczestnicy programu w coraz szerszym zakresie podejmują współpracę na szczeblu lokalnym z innymi podmiotami, w ramach organizowanych wydarzeń m.in. z urzędami miast i gmin, policją, prokuraturami, sądami, radiem, redakcjami gazet czy telewizją. Współpraca ta stanowi cenny element promocji szkoły dbającej o bezpieczeństwo uczniów.

Podczas IX edycji TDTS, 10 grudnia 2018 r. odbyło się spotkanie w Przysusze (woj. mazowieckie), pod hasłem „#RODO w edukacji. Mazowieckie spotkanie z ochroną danych

osobowych w szkole", inaugurujące cykl konferencji wojewódzkich prezentujących cele i zasady udziału w programie TDTS, placówkom oświatowym z niewielkich miejscowości.

Upowszechnienie doświadczeń i materiałów edukacyjnych wypracowanych w ciągu tych wielu lat realizacji programu, miało w zamierzeniu organu nadzorczego zachęcić inne placówki do przyłączenia się do kolejnej edycji tego przedsięwzięcia. O ile bowiem obecnie aktywne w nim są szkoły z dużych i średnich miast, o tyle placówki z mniejszych miejscowości są w nim mniej licznie reprezentowane. Stąd zorganizowane przez UODO spotkanie w Przysusze było okazją do zaprezentowania zarówno celów programu, jak i działań podejmowanych przez szkoły z tego terenu.

Porozumienie GIODO z Politechniką Śląską o współpracy w zakresie ochrony prywatności i danych osobowych – Gliwice, 5.03.2018 r.

Podczas Konferencji Rektorów Polskich Uczelni Technicznych (KRPUT), która z udziałem Mirosława Sanka, Zastępcy Generalnego Inspektora Ochrony Danych, odbyła się na Politechnice Śląskiej w Gliwicach w dniu 5.03.2018 r., podpisane zostało porozumienie o współpracy pomiędzy tą Uczelnią a GIODO o współpracy w zakresie ochrony prywatności i danych osobowych.

Porozumienie przewiduje współpracę w zakresie działalności naukowo-badawczej, edukacyjnej, promocyjnej, wydawniczej oraz organizacyjnej. W celu zapewnienia, by wiedza przekazywana w toku kształcenia była na najwyższym poziomie i zgodna ze stanowiskami organu ochrony danych osobowych w sprawach, które były przedmiotem jego rozstrzygnięć, Politechnika Śląska będzie przekazywała 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 studiów podyplomowych.

Narodowy Instytut Samorządu Terytorialnego – NIST, 29.05.2018 r.

W związku z planowanym uruchomieniem przez Prezesa UODO wspólnie z NIST kampanii edukacyjno-informacyjnej na temat stosowania nowego prawa o ochronie danych osobowych, 29 maja 2018 r. podpisano porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych. Porozumienie otwiera drogę do wspólnych działań edukacyjnych w całej Polsce, adresowanych do pracowników odpowiedzialnych za bezpieczeństwo danych osobowych samorządu terytorialnego (jst).

PORADNIKI, WYTYCZNE

Od rozpoczęcia stosowania RODO w maju 2018 roku, Prezes UODO przygotował wiele publikacji o charakterze edukacyjnym, pomocnych we właściwym rozumieniu i stosowaniu przepisów ogólnego rozporządzenia, w wybranych obszarach działalności różnych podmiotów.[211] Dotychczas ukazały się:

1. **Dwuczęściowy poradnik: „Jak rozumieć podejście oparte na ryzyku?" oraz „Jak stosować podejście oparte na ryzyku?" (maj 2018)**

Zgodnie z RODO, każdy podmiot musi samodzielnie oceniać ryzyko, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą. Ogólne rozporządzenie o ochronie danych (RODO) nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne czy zakres i rodzaj danych oraz cel ich przetwarzania. Jednym ze skutecznych systemowych sposobów dokonywania oceny ryzyka jest

[211] Organ nadzorczy wskazuje przy tym, że w wielu przypadkach, w których pojawiają się wątpliwości związane ze stosowaniem RODO, pomocne w ocenie danej sytuacji czy też – doborze odpowiednich środków ochrony danych – mogą być wytyczne Grupy Roboczej Artykułu 29, która od 25 maja 2018 roku działa jako **Europejska Rada Ochrony Danych**.

wdrożenie w danej jednostce procesu zarządzania ryzykiem. Dla ułatwienia przyjęcia w tym zakresie właściwych rozwiązań, Prezes UODO przygotował dwuczęściowy poradnik.

W pierwszej części, zatytułowanej *Jak rozumieć podejście oparte na ryzyku według RODO?*, eksperci Urzędu Ochrony Danych Osobowych wyjaśniają istotę zasady podejścia opartego na ryzyku oraz wskazują, do czego zasada ta zobowiązuje podmioty stosujące przepisy ogólnego rozporządzenia o ochronie danych. Tłumaczą też, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą. Podkreślają przy tym, **że szacowanie ryzyka to proces ciągły**, który powinien być przeprowadzany przy użyciu konkretnej metody, zapewniającej jednocześnie stosowanie jednolitych definicji i pojęć.

W drugiej części, zatytułowanej *Jak stosować podejście oparte na ryzyku?*, przedstawione zostały kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka, czyli tzw. oceny skutków dla ochrony danych.

2. „Ochrona danych osobowych w szkołach i placówkach oświatowych" – poradnik powstał we współpracy z Ministerstwem Edukacji Narodowej (sierpień 2018)

Poradnik zawiera zaktualizowane wskazówki dotyczące bezpiecznego przetwarzania danych osobowych dzieci, ich rodziców oraz opiekunów prawnych, nauczycieli, a także innych pracowników szkół i placówek oświatowych.

W opracowaniu wskazano podstawowe zasady, jakich dyrektorzy szkół i placówek oświatowych powinni przestrzegać, przetwarzając dane osobowe oraz jak stosować w praktyce przepisy ogólnego rozporządzenia w codziennej pracy placówek oświatowych. Publikacja zawiera też wiele informacji, które będą przydatne również uczniom i rodzicom.

3. „Ochrona danych osobowych w kampanii wyborczej" (sierpień 2018)

Komitety wyborcze oraz inne podmioty zaangażowane w kampanię wyborczą muszą przestrzegać nie tylko przepisów szczególnych bezpośrednio regulujących jej przebieg, ale również przepisów o ochronie danych osobowych. Co oznacza to w praktyce – wyjaśnia najnowszy poradnik przygotowany przez Prezesa Urzędu Ochrony Danych Osobowych.

Kto jest administratorem danych osobowych przetwarzanych na potrzeby wyborów i jakich obowiązków musi dopełnić? Jak prowadzić kompanię wyborczą z poszanowaniem zasad ochrony danych osobowych? Jakie prawa przysługują wyborcom? To tylko niektóre z istotnych zagadnień poruszonych w poradniku „Ochrona danych osobowych w kampanii wyborczej".

Przygotowany przez Prezesa UODO poradnik wyraźnie podkreśla przy tym, jak ważna jest rola administratora, czyli podmiotu decydującego o celach i sposobach przetwarzania danych, i wskazuje, że na różnych etapach kampanii wyborczej dane przetwarzają różni administratorzy.

W publikacji znalazło się też omówienie takich zagadnień, jak: realizacja obowiązku informacyjnego przez administratorów, prowadzenie dokumentacji przetwarzania danych, zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamianie osób o naruszeniu ochrony ich danych czy wyznaczanie inspektora ochrony danych. Poradnik wskazuje w końcu, które akty prawne regulują przebieg wyborów, w sposób szczególny akcentując kwestie związane z przetwarzaniem danych osobowych wyborców.

Poradnik został przygotowany z myślą o wszystkich podmiotach zaangażowanych w proces wyborczy – kandydatach i ich komitetach, instytucjach odpowiedzialnych za organizację i przeprowadzenie wyborów, a wreszcie samych wyborcach, których dane są przetwarzane. Ci ostatni w publikacji UODO znajdą choćby podpowiedzi, jak skorzystać z praw, jakie daje im RODO.

4. **„Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego"**

Od 25 maja 2018 r. stosowanie monitoringu wizyjnego podlega przepisom ogólnego rozporządzenia oraz regulacjom krajowym, które dotyczą m.in. pracodawców, placówek oświatowych oraz jednostek samorządu terytorialnego.

W związku z wątpliwościami interpretacyjnymi jakie zrodziły w praktyce nowe regulacje, Prezes UODO przygotował ***Wskazówki dotyczące stosowania monitoringu wizyjnego***. Dokument ten

w sposób kompleksowy omawia dopuszczalne cele stosowania monitoringu wizyjnego, prawa osób obserwowanych oraz obowiązki administratorów. Zawiera też odpowiedzi na najczęściej zadawane przez administratorów pytania.

Zgodnie z zapowiedzią dr Edyty Bielak-Jomaa, Prezesa UODO, **z końcem września upłynął okres przejściowy**, w którym organ ds. ochrony danych osobowych miał z urzędu nie podejmować działań władczych, dając podmiotom stosującym monitoring wizyjny czas na dostosowanie się do wymogów wynikających zarówno z nowych, sektorowych przepisów, jak i postanowień ogólnego rozporządzenia o ochronie danych.

Do Prezesa UODO wciąż wpływają jednak skargi, uwagi i prośby o wyjaśnienia związane ze stosowaniem monitoringu wizyjnego przez różne podmioty. Wiele ze skarg dotyczy monitoringu prowadzonego przez spółdzielnie i wspólnoty mieszkaniowe czy przedsiębiorców, niektóre z nich związane są z wykorzystywaniem monitoringu przez pracodawców. Jedna ze skarg złożonych do Prezesa UODO dotyczyła monitoringu wizyjnego w szpitalu. Niektóre ze skarg odnoszą się wreszcie do stosowania monitoringu przez osoby fizyczne. Chodzi tu o przypadki, gdy jeden z sąsiadów montuje kamery np. na balkonie czy przy swojej posesji, zaś w ich zasięgu może znajdować się nie tylko obszar jego nieruchomości, ale również nieruchomość sąsiadów, którzy sobie tego nie życzą. Wszystkie ww. sytuacje i wątpliwości zaadresowane zostaną w przygotowywanej, ostatecznej wersji tego dokumentu.

5. „Ochrona danych osobowych w miejscu pracy. Poradnik dotyczący zatrudnienia" (październik 2018)

Poradnik zawiera wskazówki, jak przetwarzać dane osobowe w procesie rekrutacji i w trakcie okresu zatrudnienia. Dokument obejmuje kwestie związane zarówno z zatrudnieniem na podstawie stosunku pracy, jak i z innymi formami zatrudnienia, w tym na podstawie umów cywilnoprawnych. Przydatne informacje znajdą tu pracodawcy, agencje zatrudnienia i pracownicy. Wiele wskazówek tu zawartych odnosi się do relacji między pracodawcą a innymi podmiotami – związkami zawodowymi, podmiotami świadczącymi usługi z zakresu medycyny pracy czy firmami szkoleniowymi.

W poradniku podkreślono konieczność zachowania przez pracodawców ostrożności przy korzystaniu z nowoczesnych technologii – które musi się odbywać przy poszanowaniu przepisów o ochronie danych osobowych. Dotyczy to w szczególności rekrutacji on-line, ewidencjonowania czasu pracy, kontrolowania poczty elektronicznej pracownika, monitorowania aktywności zatrudnionych, czy dopuszczalności korzystania z urządzeń lokalizujących pracowników.

Konferencje i seminaria

W analizowanym roku sprawozdawczym organ nadzorczy organizował konferencje i seminaria, jak również brał aktywny udział w konferencjach zorganizowanych przez inne podmioty. GIODGIODGIODO/Prezes UODO aktywnie uczestniczył w różnych wydarzeniach, a także patronował wielu przedsięwzięciom, których wykaz znajduje się w załączniku nr 2.

Poniżej przedstawione zostały przykłady niektórych wydarzeń o charakterze ogólnopolskim lub międzynarodowym z udziałem GIODO/Prezesa UODO bądź jego przedstawicieli. Ich pełny wykaz zawiera załącznik nr 3.

1. IV Ogólnopolska konferencja pt. „Podkarpacie dla biznesu", 4.01.2018 r.

Celem spotkania było przybliżenie przedsiębiorcom zagadnień prawnych związanych z pobytem cudzoziemców na terytorium RP, zmian w prawie pracy, w szczególności w kwestii niezarejestrowanej działalności i zatrudniania cudzoziemców, a także działań inspekcji transportu drogowego w tym zakresie. Organizatorami Konferencji był Oddział ZUS w Rzeszowie oraz Izba Administracji Skarbowej w Rzeszowie. Przedstawiciel GIODO w swoim wystąpieniu omówił kwestie związane z ochroną danych osobowych w kontekście współpracy transgranicznej.

2. XII Dzień Ochrony Danych Osobowych – 29 stycznia 2018 r.

28 stycznia już po raz dwunasty obchodzony był Dzień Ochrony Danych Osobowych. Ustanowiony dla upamiętnienia rocznicy otwarcia do podpisu najstarszego aktu prawnego o zasięgu

międzynarodowym, kompleksowo regulującego zagadnienia związane z ochroną danych osobowych, tj. Konwencji 108 Rady Europy z 28 stycznia 1981 r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych. W ten sposób Komitet Ministrów Rady Europy postanowił zwrócić uwagę na problem ochrony danych osobowych, w tym na prawa, które przy przetwarzaniu danych osobowych przysługują każdemu z nas. W całej Europie Dzień Ochrony Danych Osobowych obchodzony jest w tym samym czasie. Z tej okazji organizowane są różne wydarzenia informujące obywateli w zakresie ich praw i obowiązków oraz zagrożeń związanych z przetwarzaniem danych osobowych.

RODO było tematem przewodnim XII Dnia Ochrony Danych Osobowych

Z tej okazji odbyły się różne wydarzenia poświęcone aktualnym zagadnieniom związanym z prawem do prywatności i ochrony danych osobowych.

Główne obchody – 29 stycznia 2018 r.

Główne obchody Dnia Ochrony Danych Osobowych – organizowane przez GIODO – odbyły się 29 stycznia 2018 r. w Warszawie. Ich głównym punktem była konferencja „Zainwestuj w prywatność. Przygotowujemy się do #RODO", poświęcona praktycznym aspektom wdrożenia RODO. Podczas spotkania eksperci GIODO oraz zaproszeni praktycy wskazywali, jak poradzić sobie ze stosowaniem wielu nowych zadań, jakie na administratorów nakładają przepisy RODO, jak np.: zgłaszanie naruszeń, uwzględnianie ochrony danych w fazie projektowania czy ocena skutków dla ochrony danych.

Kalendarium wydarzeń towarzyszących

Wzorem lat ubiegłych, GIODO zaprosił do współorganizacji tego święta uczelnie wyższe, z którymi ma zawarte porozumienia o współpracy. Uczelnie te włączyły się w obchody XII Dnia, organizując liczne spotkania i konferencje z udziałem ekspertów GIODO. Na obchody XII Dnia Ochrony Danych Osobowych złożyły się następujące wydarzenia:

- **Kraków, 22 stycznia 2018 r.** – konferencja pt. „RODO, nowe przepisy, nowe obowiązki, nowy zawód", zorganizowana przez Akademię Ignatianum w Krakowie.
- **Łódź, 30 stycznia 2018 r.** – ogólnopolska konferencja naukowa „Administrator danych osobowych w perspektywie RODO", zorganizowana przez Centrum Ochrony Danych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.
- **Warszawa, 30 stycznia 2018 r.** – ogólnopolska konferencja pt. „ABI w nowej roli – inspektor ochrony danych". Organizatorzy: Stowarzyszenie Administratorów Bezpieczeństwa Informacji (SABI) oraz Wydział Zarządzania Politechniki Warszawskiej.
- **Dąbrowa Górnicza, 1 lutego 2018 r.** – „Dzień Otwarty Generalnego Inspektora Ochrony Danych Osobowych 2018" w Wyższej Szkole Biznesu w Dąbrowie Górniczej, podczas którego odbyła się konferencja tematyczna dotycząca nowej roli i praktycznych aspektów pracy administratorów bezpieczeństwa informacji w świetle ogólnego rozporządzenia o ochronie danych, a także kwestii dostosowania ochrony danych osobowych w placówkach oświatowych do wymogów RODO. W czasie trwania konferencji czynne były stoiska, przy których eksperci (m.in.z GIODO) udzielali bezpłatnych porad prawnych i informacji z zakresu ochrony danych osobowych oraz rozdawali materiały edukacyjno-informacyjne.
- **Kraków, 2 lutego 2018 r.** – Konferencja dla Dyrektorów Szkół Ćwiczeń pt. „Ochrona danych osobowych w placówkach oświatowych w świetle RODO", zorganizowana przez Uniwersytet Pedagogiczny im. KEN w Krakowie.
- **Warszawa, 15 lutego 2018 r.** – konferencja „Od ustawy ODO do RODO". Organizatorzy: Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi Collegium Civitas oraz nFlo Sp. z o.o.
- **Wrocław, 21 lutego 2018 r.** – konferencja „Aktualny stan przygotowania polskiego systemu prawnego do bezpośredniego stosowania RODO – postulaty de lege ferenda". Organizator: Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.
- **Warszawa, 26 lutego 2018 r.** – wystąpienie GIODO podczas posiedzenia Senatu Warszawskiego Uniwersytetu Medycznego.

- **Szczytno, 27–28 lutego 2018 r.** – konferencja naukowa „Udział Policji oraz innych służb i instytucji w ochronie infrastruktury krytycznej Państwa w dobie niesymetrycznych zagrożeń. Diagnoza i perspektywy" zorganizowana przez Wyższą Szkołę Policji w Szczytnie we współpracy z GIODO.
- **Gdynia, 28 lutego 2018 r.** – konferencja „Bezpieczeństwo danych osobowych w cyberprzestrzenie szanse, wyzwania, zagrożenia". Organizatorzy: Akademia Marynarki Wojennej, Uniwersytet Humanistyczny w Siedlcach, Wyższa Szkoła Policji w Szczytnie, Wojskowa Akademia Techniczna, Zespół Zarządzania Wsparciem Teleinformatycznym w Gdyni, Centralna Biblioteka Wojskowa, Wojskowy Instytut Łączności oraz GIODO.

3. Konferencja „Bezpieczeństwo informacji w sektorze ochrony zdrowia", 1.03.2018 r.

Podtytułem tematycznym konferencji było „Wdrożenie rozporządzenia RODO w sektorze ochrony zdrowia". Wydarzenie to koncentrowało się na zmianie systemu ochrony danych osobowych w Polsce. Celem konferencji było przedstawienie zagrożeń w zakresie bezpieczeństwa informacji oraz zaprezentowanie konkretnych rozwiązań technicznych i organizacyjno-prawnych, minimalizujących ryzyka z zakresu bezpieczeństwa informacji. Reformie prawa o ochronie danych osobowych, z uwzględnieniem wpływu na sektor ochrony zdrowia, poświęcone były wystąpienia przedstawicieli GIODO. Organizatorem wydarzenia był Śląski Uniwersytet Medyczny w Katowicach, z którym organ ds. ochrony danych osobowych współpracuje nad kodeksem postępowania w świetle RODO dla sektora zdrowia.

4. Konferencja Rektorów Polskich Uczelni Technicznych, 5.03.2018 r.

Organ właściwy do spraw ochrony danych osobowych jest częstym gościem odbywających się cyklicznie kilka razy w roku Konferencji Rektorów Polskich Uczelni Technicznych – KRPUT. Podczas tych spotkań podejmowane zagadnienia ważne z punktu widzenia przetwarzania danych osobowych w działalności szkół wyższych, w szczególności tych o profilu technicznym.

W 2018 r. Mirosław Sanek, Zastępca Generalnego Inspektora Ochrony Danych Osobowych wystąpił w sesji poświęconej tematyce bezpieczeństwa danych w świetle zbliżającego się terminu rozpoczęcia stosowania nowego prawa o ochronie danych. Gospodarzem KRPUT była Politechnika Śląska. Podczas wydarzenia podpisane zostało porozumienie pomiędzy Politechniką Śląską a GIODO o współpracy w zakresie ochrony prywatności i danych osobowych.

5. Sympozjum Naukowe „Prawo do prywatności w Kościołach i innych związkach wyznaniowych: od tajemnicy duszpasterskiej do ochrony danych osobowych". Warszawa, 15.03.2018 r.

15 marca 2018 r. Chrześcijańska Akademia Teologiczna w Warszawie wspólnie z Polską Radą Ekumeniczną i Polskim Towarzystwem Prawa Wyznaniowego zorganizowała Sympozjum Naukowe „Prawo do prywatności w Kościołach i innych związkach wyznaniowych: od tajemnicy duszpasterskiej do ochrony danych osobowych". Przedsięwzięcie to związane było ze zbliżającym się terminem rozpoczęcia stosowania RODO w polskim porządku prawnym.

Przepisy nowego prawa o ochronie danych osobowych zawierają kwestie odgrywające ważną rolę w legislacji wewnętrznej i w praktyce kościołów i innych związków wyznaniowych. Organizatorzy przygotowali na obrady wzorcowy projekt aktu prawa wewnętrznego, zawierającego szczegółowe zasady przetwarzania i ochrony danych osobowych w związkach wyznaniowych. Podczas sympozjum omówiono zagadnienia dotyczące ochrony tajemnicy spowiedzi (względnie tajemnicy duszpasterskiej) oraz ochrony danych osobowych w Kościele kontekście konstytucyjne chronionych autonomii i niezależności związków wyznaniowych.

6. IV Forum Prawa Mediów Elektronicznych, 10–11.04.2018 r.

Konferencja poświęcona była zagadnieniom związanym z ochroną danych osobowych na gruncie ogólnego rozporządzenia, w szczególności tych na styku prawa i nowych technologii informatycznych i elektronicznych. Celem spotkania było pogłębienie integracji środowiska skupionego wokół problematyki prawa mediów elektronicznych oraz cyfryzacji administracji publicznej, ochrony danych osobowych, bankowości oraz e-zdrowia. Organizatorem Konferencji było Centrum Badań Problemów

i Ekonomicznych Komunikacji Elektronicznej Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

7. XXIX Ogólnopolska konferencja Uniwersyteckich Poradni Prawnych, 14.04.2018 r.

Organizatorem wydarzenia była Studencka Poradnia Prawa przy Collegium Polonicum w Słubicach, będącym wspólną placówką naukowo-badawczą Uniwersytetu im. Adama Mickiewicza w Poznaniu i Europejskiego Uniwersytetu Viadrina we Frankfurcie nad Odrą. Tematem przewodnim Konferencji była ochrona danych osobowych i mediacja interdyscyplinarna, zaś jej celem prezentacja badań i osiągnięć naukowych z zakresu ochrony danych osobowych oraz mediacji, a także wymiana poglądów i doświadczeń z działalności poszczególnych poradni prawnych w Polsce – m.in. poprzez warsztaty nt. doskonalenia umiejętności niezbędnych w komunikowaniu się z klientem. Jeden z warsztatów poświęcony został ochronie danych osobowych w kontekście zbliżającej się daty rozpoczęcia obowiązywania unijnego ogólnego rozporządzenia o ochronie danych. Zajęcia w ramach tego warsztatu poprowadzili przedstawiciele GIODO. Konferencja ta połączona była z obchodami 15-lecia działalności Studenckiej Poradni Prawnej w Słubicach.

8. X Międzynarodowa Konferencja Naukowa „Powszechne i regionalne systemy ochrony praw człowieka 70 lat po proklamowaniu Powszechnej Deklaracji Praw Człowieka", 23.04.2018 r.

Wydział Prawa, Administracji i Zarządzania Uniwersytetu Jana Kochanowskiego w Kielcach, we współpracy z Zarządem Głównym Stowarzyszenia Parlamentarzystów Polskich, zorganizował w Sejmie RP międzynarodową konferencję upamiętniającą 70.rocznicę proklamowania Powszechnej Deklaracji Praw Człowieka. Wystąpienie otwierające wygłosił Mirosław Sanek, Zastępca GIODO. W Konferencji uczestniczyli parlamentarzyści i przedstawiciele środowisk naukowych z Polski, Białorusi, Hiszpanii, Litwy, Niemiec, Rosji, Serbii, Słowacji, USA oraz Ukrainy.

9. XII Ogólnopolska Konferencja Społeczności Centrum Europejskiego Uniwersytetu Warszawskiego, 27.04.2018 r.

„Wojny w czasach cyfrowej rewolucji" nosiła tytuł Ogólnopolska Konferencja Społeczności Centrum Europejskiego, która z udziałem przedstawiciela UODO odbyła się na Uniwersytecie Warszawskim. Przemiany dokonujące się w Europie i na świecie związane z rozwojem nowoczesnych technologii wymuszają na rządach określone działania w kierunku zapewnienia cyberbezpieczeństwa i prowadzenie polityki obronnej ukierunkowanej na przeciwdziałanie wirtualnym zagrożeniom dla prawa do prywatności i ochrony danych osobowych. Dyskusji podczas Konferencji przyświecało fundamentalne pytanie, czym dla obywatela jest bezpieczeństwo, ile jesteśmy w stanie oddać, by czuć się bezpieczniej i jak brzmi nowa definicja obrony narodowej w erze cyfrowej.

10. X Konferencja Naukowa „Bezpieczeństwo w Internecie", 25.05.2018 r.

Konferencja została zorganizowana w ramach X edycji corocznych interdyscyplinarnych debat nad bezpieczeństwem w Internecie, które nieprzerwanie od dziesięciu lat odbywają się z udziałem przedstawicieli organu ochrony danych osobowych. GIODO był współorganizatorem wszystkich poprzednich edycji tego cyklicznego wydarzenia. Tegoroczna, X edycja, zbiegła się z datą wejścia w życie RODO i rozpoczęciem stosowania tego aktu prawnego w polskim porządku prawnym.

11. Konferencja Wyższych Przełożonych Zakonów Męskich w Polsce, 11–13.06.2018 r.

Przedstawiciele UODO uczestniczyli w spotkaniu sekretarzy i ekonomów w kieleckiej Konferencji Wyższych Przełożonych Zakonów Męskich w Polsce, oraz wystawie SACROEXPO. Podczas wydarzenia jego uczestnicy przedstawili zagadnienia związane z ochroną danych osobowych w relacji RODO – prawo wewnętrzne Kościoła katolickiego oraz aktualne wymagania dotyczące ochrony danych osobowych w cyberprzestrzeni. Konferencja odbyła się w ramach współpracy UODO z Kościelnym Inspektorem Ochrony Danych.

12. V Ogólnopolskie Seminarium Sekretarzy, 27.06.2018 r.

Spotkanie zostało zorganizowane dla sekretarzy, kadry zarządzającej, przedstawicieli działów organizacyjnych, kadr i płac, IT, osób odpowiedzialnych za procesy informatyczne w urzędach, IOD oraz radców prawnych obsługujących samorządy. Przedstawiciel UODO wystąpił w dyskusji panelowej „RODO – praktyczne wskazówki dla działów kadr w urzędach", podczas której przybliżył zagadnienia

związane z RODO w działalności jednostek samorządu terytorialnego, w szczególności w kontekście organizacji wyborów oraz powszechnej cyfryzacji usług publicznych. Współorganizatorem wydarzenia była redakcja Pisma Samorządu Terytorialnego „WSPÓLNOTA".

13. XXII Konferencja „Miasta w Internecie", 27–29.06.2018 r.

XXII Konferencja z cyklu „Miasta w Internecie" odbyła się pod hasłem „ROK 2018: PUZZLE CYFROWEJ POLSKI – Miasta przyszłości – Technologie Transformacji – Cyfrowa Szkoła". Przedstawiciel UODO wystąpił w jednym z paneli z prezentacją na temat przepisów ogólnego rozporządzenia w kontekście koniecznych zmian w urzędach administracji samorządowej. Konferencja „Miasta w Internecie" gromadzi co roku przedstawicieli rządu, samorządów lokalnych i regionalnych, a także przedstawicieli świata nauki, organizacji pozarządowych i firm sektora ICT. Tworzy w ten sposób przestrzeń dla debaty nad wpływem i odpowiedzialnością władz publicznych za rozwój cyfrowy kraju.

14. Międzynarodowa Konferencja „Prawa człowieka: ewaluacja i kierunki rozwoju", 3–4.07.2018 r., Warszawa

W siedzibie UKSW w Warszawie odbyła się Międzynarodowa Konferencja „Prawa człowieka: ewaluacja i kierunki rozwoju", której współorganizatorami byli Prezes UODO, Uniwersytet Kardynała Stefana Wyszyńskiego, Uniwersytet Warszawski oraz International Centre on Law, Life, Faith and Family. Patronat honorowy nad wydarzeniem objął Minister Spraw Zagranicznych w ramach obchodów 25-lecia Europejskiej Konwencji Praw Człowieka w Polsce. Podczas sesji plenarnej „Ochrona danych osobowych i prywatności. Idea *good governance*", przedstawiciel UODO wygłosił przemówienie pt. „Relacja między orzecznictwem Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej".

15. Warsztat dyskusyjny dotyczący stosowania monitoringu wizyjnego, 18.07.2018 r.

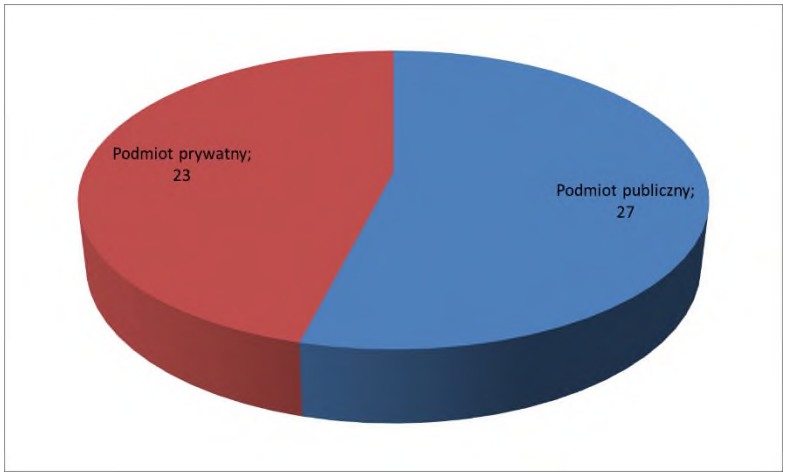
Warsztat nt. stosowania monitoringu wizyjnego, który z inicjatywy Prezesa UODO odbył się 18.07.2018 r. w Warszawie, był rezultatem zakończonych 15.07.2018 r. konsultacji społecznych, podczas których zbierane były uwagi i sugestie dotyczące problemów wynikających ze stosowania monitoringu wizyjnego.

Warsztat cieszył się bardzo dużym zainteresowaniem – uczestniczyło w nim bowiem ponad 200 osób reprezentujących zarówno administrację publiczną, jak i izby gospodarcze, przedsiębiorców, a także organizacje społeczne. Wzięli w nim również udział przedstawiciele Rzecznika Praw Obywatelskich, Rzecznika Praw Dziecka oraz Najwyższej Izby Kontroli.

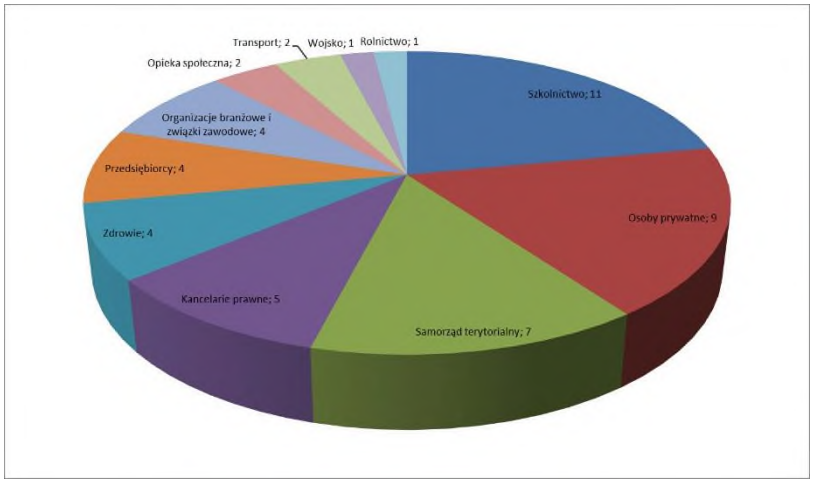
Uczestnicy warsztatu zgłosili wiele praktycznych problemów, z którymi stykają się na co dzień w swojej pracy. Wskazywali na wątpliwości, jakie rodzą się w związku ze stosowaniem monitoringu np. przez spółdzielnie mieszkaniowe czy osoby prywatne. Podnoszono różne aspekty związane z prawami osób, które zostały uchwycone przez oko kamery. Postulowano też, by we wskazówkach Prezesa UODO omówić zagadnienia monitoringu w obiektach należących do tzw. infrastruktury krytycznej, tj. w obiektach ważnych dla państwa i obywateli. Wskazano, że cennym uzupełnieniem wskazówek byłoby też uwzględnienie monitoringu prowadzonego z wykorzystaniem nowych technologii, m.in sztucznej inteligencji, czy rozwiązań opartych na rozpoznawaniu twarzy i analizie zachowań.

Konsultacje, jak i warsztat je podsumowujący dowiodły, że tematyka monitoringu wizyjnego jest złożona, a wiele kwestii wciąż budzi wątpliwości i wymaga jeszcze dokładniejszego wyjaśnienia. Z tego powodu „Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego" zostaną uzupełnione. Będzie to możliwe dzięki uwagom zgłoszonym zarówno w toku konsultacji, jak i podczas warsztatu.

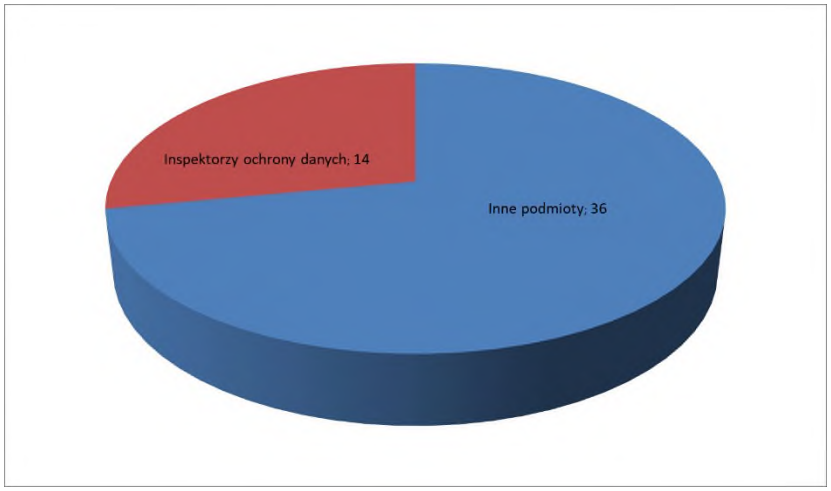
Konsultacje w liczbach



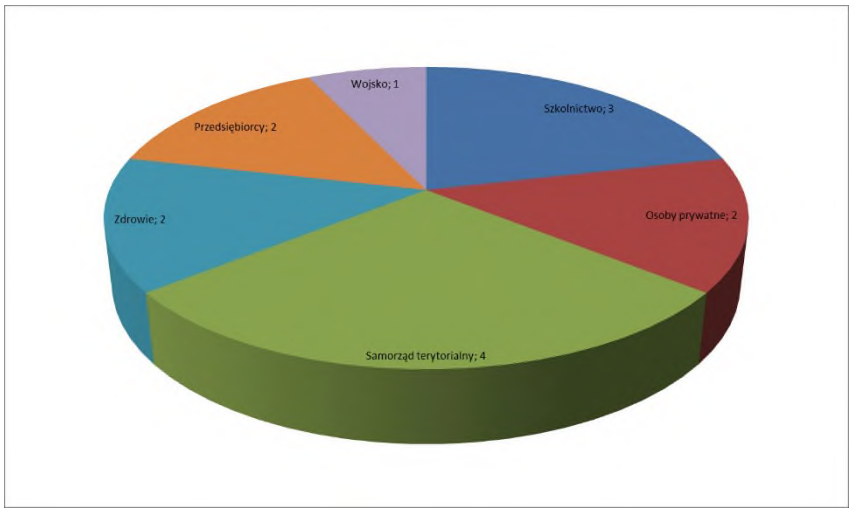
Wykres 1. *Podział uczestników konsultacji na sektor prywatny i publiczny.*



Wykres 2. *Podział uczestników konsultacji.*



Wykres 3. *Udział inspektorów ochrony danych (IOD) na tle wszystkich uczestników.*



Wykres 4. *Podział inspektorów ochrony danych według sektorów*.

16. XXVIII Forum Ekonomiczne w Krynicy Zdroju, 4–6.09.2018 r.

„Europa wspólnych wartości czy Europa wspólnych interesów?" – pod takim tytułem odbyło się XXVIII Forum Ekonomiczne w Krynicy Zdroju, zorganizowane przez Instytut Studiów Wschodnich. Forum Ekonomiczne to miejsce dyskusji nad ważnymi kwestiami dotyczącymi energetyki, makroekonomii i bezpieczeństwa międzynarodowego, z udziałem przedstawicieli elit naukowych, politycznych, gospodarczych, kulturalnych oraz mediów z państw Europy, Azji oraz Ameryki Północnej. Podczas tego wydarzenia dr Edyta Bielak-Jomaa, Prezes UODO, przedstawiła zasady nowego prawa o ochronie danych osobowych w kontekście wyzwań dla sektora publicznego i prywatnego oraz pierwsze doświadczenia związane z trzymiesięcznym okresem stosowania RODO.

17. Seminarium Naukowe „Ochrona danych osobowych w fazie projektowania. Wymogi RODO w tworzeniu oprogramowania". Warszawa, 21.09.2018 r.

Prezes UODO był organizatorem seminarium naukowego adresowanego do programistów i twórców oprogramowania. Wydarzenie to zaplanowane zostało z myślą o osobach uczestniczących w procesach wytwarzania oprogramowania, tj. programistach i architektach oprogramowania, osobach biorących udział w specyfikowaniu wymagań i odbieraniu systemów informatycznych, w szczególności zaś o tych, którzy są zainteresowani tworzeniem systemów i programów zgodnych ze standardami wprowadzonymi przez RODO.

RODO doprecyzowało wiele kwestii znajdujących się na styku zagadnień związanych z tworzeniem oprogramowania a bezpieczeństwem danych osobowych. Programiści w swojej pracy wykorzystują różnorodne wzorce projektowe oraz zestawy dobrych praktyk, dzięki którym znacząco zmniejszają ryzyko pominięcia istotnych elementów oraz skracają czas pracy nad oprogramowaniem. Podobnie można też rozumieć niektóre wytyczne wynikające z RODO.

Uczestnicy seminarium mogli wziąć udział w dyskusji na temat aktualnej sytuacji prawnej dotyczącej ochrony danych osobowych, ze szczególnym uwzględnieniem jej wpływu na systemy informatyczne. Podczas seminarium szeroko omówione zostały m.in. zasady data protection by default, czyli domyślnego ustawiania wysokiego poziomu ochrony danych osobowych, data protection by design, polegająca na uwzględnieniu ochrony danych w fazie projektowania, zagadnienia pseudonimizacji i anonimizacji, a także metody szacowania ryzyka i ocena skutków dla ochrony danych. Spotkanie to było okazją do zaprezentowania praktycznych przykładów, jak poprawnie implementować przepisy RODO z perspektywy tworzenia oprogramowania, które musi

być też zgodne z wymaganiami dla użytkowników zewnętrznych, a także dla IOD oraz pracowników podmiotu, dla którego powstało.

18. Ogólnopolska Konferencja Naukowa „Pozycja prawna inspektora ochrony danych", Łódź, 28.09.2018 r.

Celem konferencji było zwrócenie uwagi na problemy związane z pozycją prawną inspektora ochrony danych osobowych w świetle RODO, w ujęciu prawnoporównawczym. Podczas tego wydarzenia przedstawiciele UODO zaprezentowali nowe podejście do ochrony danych w związku z wykonywaniem funkcji IOD, kompetencje i umiejętności, jakimi powinien wykazać się IOD w świetle możliwych mechanizmów certyfikacji, a także sposób wykazania przez administratora przestrzegania RODO – w oparciu o prowadzoną dokumentację. Organizatorem wydarzenia było Centrum Ochrony Danych Osobowych i Zarządzania Informacją na działające Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.

19. IV Ogólnopolski Szczyt Gospodarczy – OSG 2018, 18–19.10.2018 r.

Europejskie Centrum Biznesu było organizatorem odbywającego się w Siedlcach IV Ogólnopolskiego Szczytu Gospodarczego pt. „Państwo – Gospodarka – Bezpieczeństwo: filary polskiej gospodarki przyszłości". Dr Edyta Bielak-Jomaa, Prezes UODO, oraz przedstawiciel UODO byli uczestnikami panelu poświęconego gospodarce, podczas którego poruszony był temat RODO w kontekście wsparcia czy utrudnienia w prowadzeniu biznesu.

IV Szczyt koncentrował się na filarach polskiej gospodarki przyszłości, czyli na tych branżach, firmach czy instytucjach, które swoją determinacją przyczyniły się do rozwoju gospodarczego kraju. Debata prowadzona była pod kątem zabezpieczenia polskiej gospodarki pod kątem ryzyk wynikających z sytuacji międzynarodowej, otoczenia makroekonomicznego, bezpieczeństwa (gospodarczego, energetycznego, finansowego), jak również potencjału infrastrukturalnego i innowacyjnego.

20. II Konferencja Naukowa „Bezpieczeństwo dokumentów publicznych", 19.10.2018 r.

Konferencje organizowane cyklicznie przez MSWiA są elementem kampanii informacyjno-szkoleniowej dotyczącej zagadnień związanych z budowanym w Polsce systemem bezpieczeństwa dokumentów. Uchwalona przez Sejm RP kilka dni wcześniej, tj. 4 października 2018 r. ustawa o dokumentach publicznych, była odpowiedzią na sygnalizowaną od lat potrzebę uporządkowania tego obszaru działalności publicznej RP.

W trakcie prac nad tą ustawą, organ właściwy w sprawie ochrony danych osobowych, konsekwentnie podtrzymywał swoje stanowisko w kwestii utworzenia **państwowego elektronicznego systemu umożliwiającego łatwe i szybkie zgłaszanie przez obywateli utraty dokumentów tożsamości.** Z praktyki UODO wynikało bowiem, że istniejące obecnie systemy zarządzane przez podmioty komercyjne (np. system „Dokumenty Zastrzeżone" Związku Banków Polskich), czy też opublikowany na stronie internetowej MSWiA wykaz unieważnionych dowodów osobistych, do których – po uwierzytelnieniu – każdy ma dostęp, w opinii organu nie są wystarczające dla zapewnienia pełnej ochrony danych osób, których dotyczą. Niemniej, postulat ten – tak ważny z punktu widzenia zapewnienia przestrzegania prawa do prywatności i ochrony danych osobowych – nie został uwzględniony w przepisach tej ustawy.

2. Działalność informacyjna

Podobnie jak w latach ubiegłych GIODO, później Prezes UODO, w 2018 r. korzystał z różnorodnych kanałów komunikacyjnych, aby upowszechniać informacje na temat systemu ochrony danych osobowych – od spotkań prasowych, poprzez udzielanie wywiadów i odpowiedzi na pytania dziennikarzy z mediów tradycyjnych i elektronicznych, aż po publikację artykułów przygotowanych przez ekspertów UODO.

Wiele informacji do mediów docierało także za pośrednictwem strony internetowej. Należy zaznaczyć, że do 24 maja 2018 r. strona była dostępna pod adresem:www.giodo.gov.pl, a następnie zastąpiła ją strona: www.uodo.gov.pl.

W 2018 r. działania informacyjne zdominowane zostały przez temat ogólnego rozporządzenia o ochronie danych osobowych (RODO).

UODO rozpowszechnił ponad 100 komunikatów w postaci informacji prasowych o tematyce ochrony danych, którymi zainicjował w mediach wiele publikacji. Większość z nich jest dostępna na stronie internetowej www.giodo.gov.pl, a teraz www.uodo.gov.pl. Dziennikarze skierowali do rzecznika prasowego 276 zapytań. GIODO/Prezes UODO wraz z ekspertami GIODO/UODO udzielili ponad 100 wywiadów.

W sumie w okresie sprawozdawczym w mediach tradycyjnych i na portalach internetowych na temat działalności najpierw GIODO, a potem UODO, ukazało się w 2018 r. blisko 12 000 informacji.

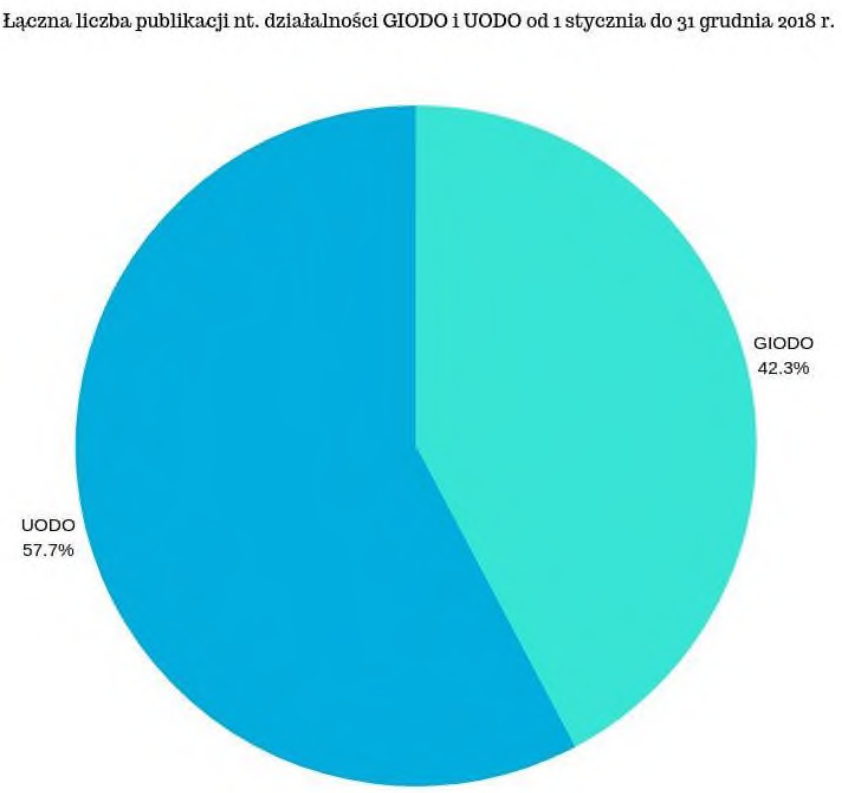
2.1. Stała współpraca z mediami

W 2018 r. współpraca z mediami skupiła się na upowszechnianiu wśród dziennikarzy wiedzy zarówno na temat RODO, w związku z rozpoczęciem 25 maja 2018 r. jego stosowania, jak i realizacji nowych zadań Prezesa UODO. Poza tym dziennikarze byli informowani o wielu innych rezultatach działań, które realizował najpierw GIODO, a potem Prezes UODO (wydawane decyzje, wyniki kontroli, przedsięwzięcia edukacyjne). Liczne informacje prasowe oraz komunikaty, które towarzyszyły różnorodnym wydarzeniom, po dotarciu do mediów były wykorzystywane bezpośrednio przez dziennikarzy lub inspirowały ich do tworzenia materiałów problemowych.

Stała współpraca z mediami obejmowała zarówno z prasę codzienną o zasięgu lokalnym i ogólnopolskim, np. dziennik „Rzeczpospolita", „Dziennik Gazeta Prawna", „Puls Biznesu" i „Gazeta Wyborcza", jak i ogólnopolskimi pismami branżowymi (m.in. „IT w Administracji", „Gazeta Ubezpieczeniowa"), a także portale internetowe (np. Dziennik Internautów, Prawo.pl, Niebezpiecznik.pl, Money.pl, WP.pl, Interia.pl).

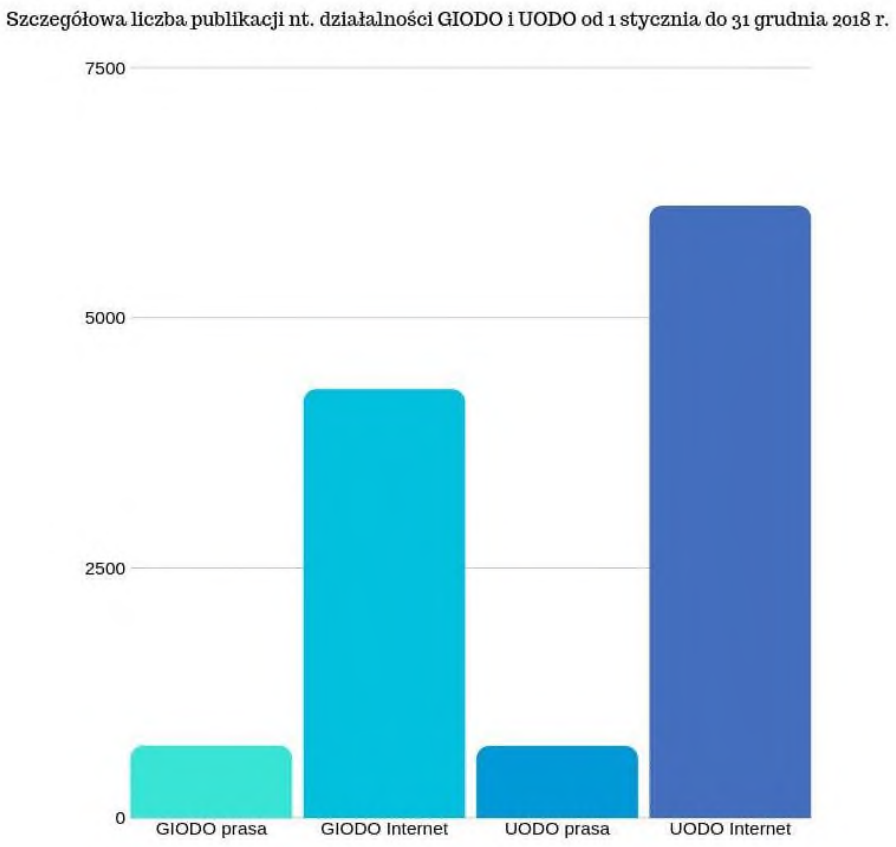
Kontynuowana była również dotychczasowa współpraca ze stacjami telewizyjnymi i radiowymi, m.in. z Polskim Radiem Jedynką, Polskim Radiem 24 czy TVP INFO, TVN24 BiS.

Łącznie w mediach drukowanych i internetowych na temat działalności najpierw GIODO, a potem UODO, **ukazało się w 2018 r. blisko 12 000 artykułów**. Szczególne nasilenie działań nastąpiło w II i III kwartale 2018 r., a więc w czasie poprzedzającym moment rozpoczęcia stosowania RODO i tuż po tym wydarzeniu.



Wykres 1. Łączna liczba publikacji nt. działalności GIODO i UODO od 1 stycznia do 31 grudnia 2018 r.

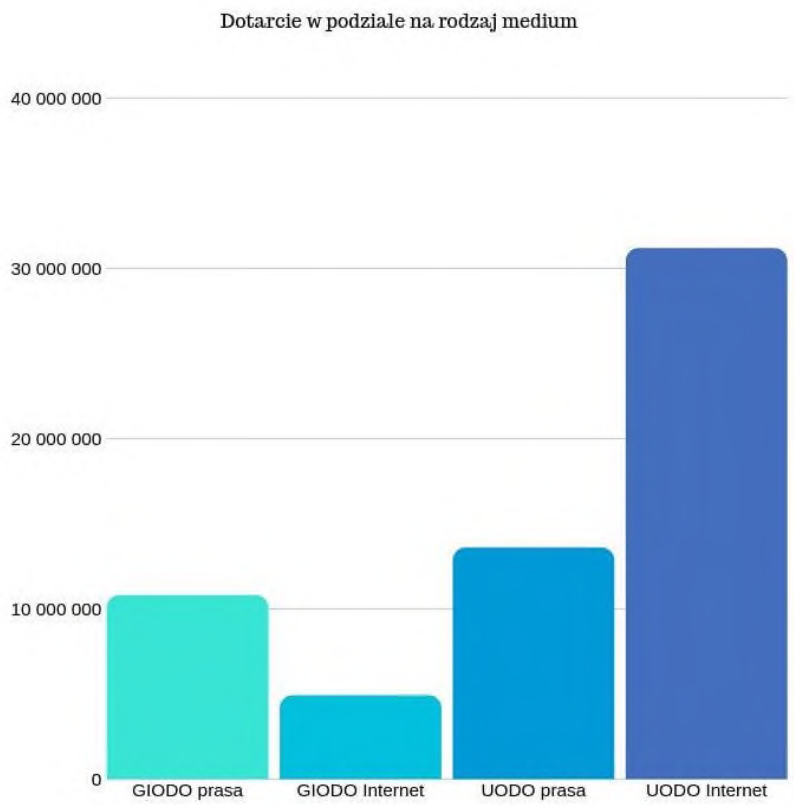
W okresie działalności GIODO, a więc od 1 stycznia do 24 maja 2018 r. ukazało się 4998 informacji na temat działań wtedy jeszcze GIODO (718 w prasie oraz 4280 w Internecie). Z kolei po 25 maja 2018 r. już na temat Prezesa UODO i Urzędu ukazało się 6 830 artykułów (716 w prasie, a 6114 na Internecie).



Wykres 2. Szczegółowa liczba publikacji nt. działalności GIODO i UODO od 1 stycznia do 31 grudnia 2018 r.

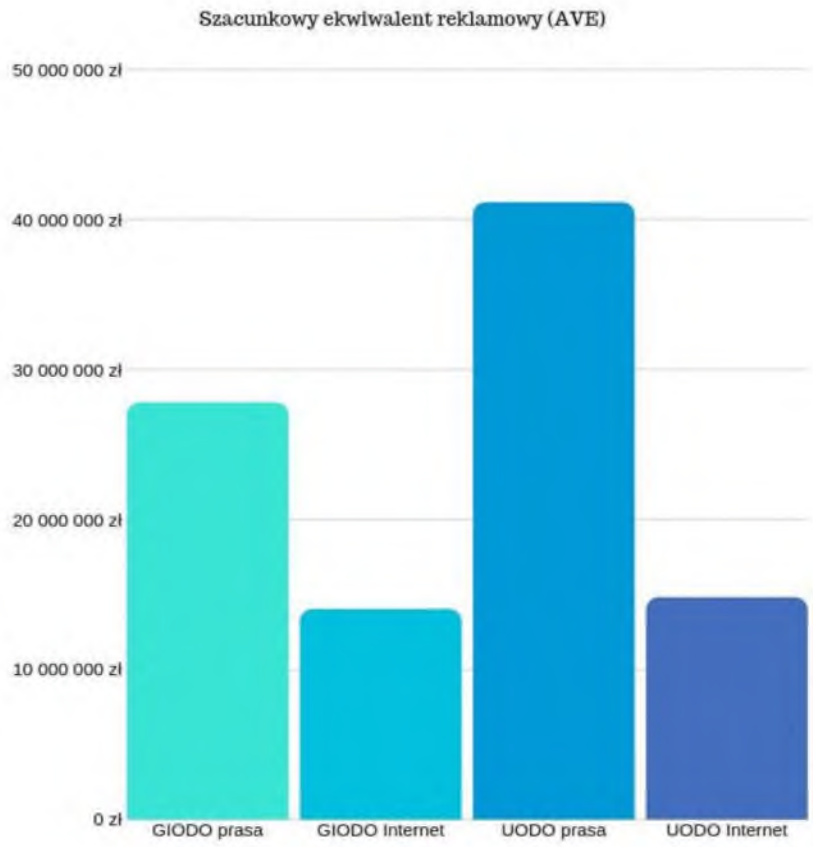
W okresie sprawozdawczym rozwijano także współpracę w postaci publikacji cyklicznych materiałów eksperckich z takimi czasopismami specjalistycznymi i branżowymi, jak: „ABI Expert", „Informacja w Administracji Publicznej", „Ochrona Danych Osobowych" czy „Monitor Prawa Pracy i Ubezpieczeń".

Dzięki tym działaniom w 2018 r. suma dotarcia do odbiorców wyniosła pod 60 mln osób, z czego ponad 24 mln to prasa drukowana, a ponad 36 mln Internet.

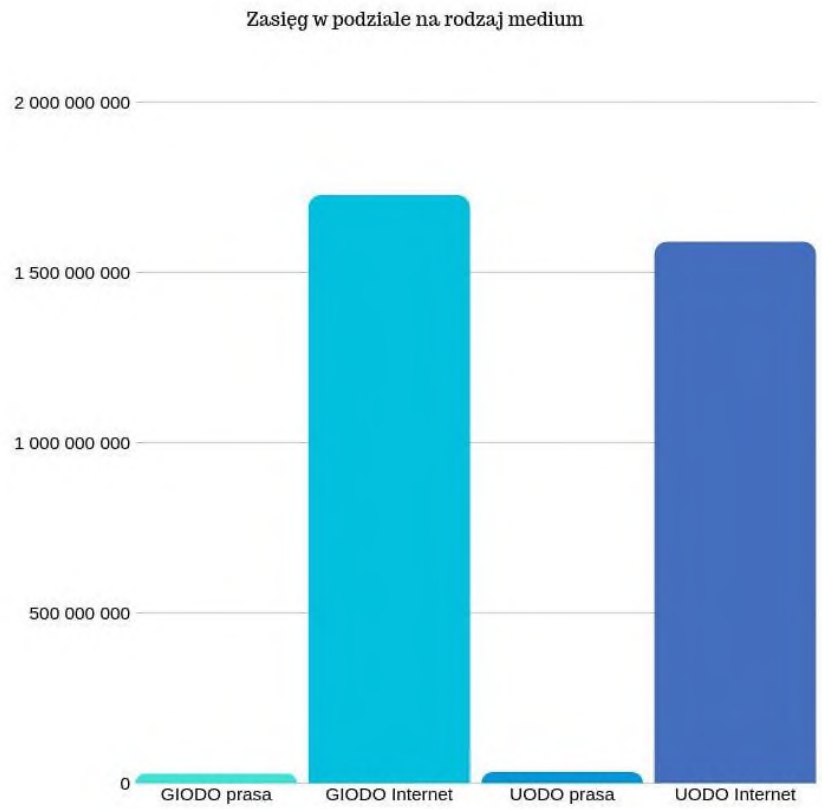


Wykres 3. Dotarcie w podziale na rodzaj medium.

Warto wspomnieć, że **wartość szacunkowego ekwiwalentu reklamowego (AVE) w odniesieniu do wskazanej sumy dotarcia wyniosła ponad 97 mln zł.** Zatem taką kwotę musiałby wydać GIODO/Prezes UODO na działania reklamowe, gdyby chciał w taki sposób dotrzeć do opinii publicznej.



Wykres 4. Szacunkowy ekwiwalent reklamowy (AVE).



Wykres 5. Zasięg

2.2. Strona internetowa i media społecznościowe

W okresie sprawozdawczym działania informacyjne prowadzone były również za pośrednictwem strony internetowej (do 24 maja 2018 r. pod adresem www.giodo.gov.pl, a od 25 maja 2018 r. – www.uodo.gov.pl). **Co miesiąc odnotowywano średnio ponad 450 tys. osłon.** Świadczy to o dużym zainteresowaniu internautów informacjami dostarczanymi opinii publicznej poprzez witrynę internetową.

Łącznie udostępniano na stronie Urzędu ponad 170 materiałów o różnych charakterze. Były to m.in. komunikaty dotyczące m.in. wytycznych i stanowisk najpierw GIODO, a następnie Prezesa UODO, relacji z wydarzeń z udziałem Prezesa UODO (wcześniej GIODO) lub inicjatyw podejmowanych przez Urząd.

W 2018 r. ogromnym zainteresowaniem cieszyły się, udostępnione prze witrynę internetową, poradniki i wytyczne poświęcone wybranym zagadnieniom stosowania RODO, jak również wszelkie komunikaty na temat praktycznych aspektów stosowania tego rozporządzenia. Ponadto działania informacyjne były także systematycznie prowadzone za pośrednictwem mediów społecznościowych – Twittera oraz YouTuba. Internauci chętnie korzystali z udostępnianych im tymi kanałami filmów edukacyjnych, transmisji wydarzeń, np. szkoleń dla IOD, a także uczestniczyli w wykładach otwartych (dostępnych w ramach IX edycji programu edukacyjnego „Twoje Dane – Twoja Sprawa).

2.3. Odpowiedzi na indywidualne pytania dziennikarzy

Współpraca z przedstawicielami mediów tradycyjnych i elektronicznych w 2018 r. koncentrowała się również na udzielaniu odpowiedzi na pytania dziennikarzy z redakcji ogólnopolskich i lokalnych, a także branżowych. **W okresie sprawozdawczym dziennikarze skierowali do Rzecznika Prasowego 276 pytań.**

Wśród problemów, którymi interesowali się przedstawiciele mediów, były m.in.:

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii,
- wykorzystywanie danych osobowych na potrzeby marketingu, ze szczególnym uwzględnieniem telemarketingu,
- udostępnienie 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 wypożyczony sprzęt sportowy, jak np. narty, łyżwy,
- wykonywanie kopii dokumentów tożsamości przez różne podmioty,
- odmowa udostępniania informacji publicznej, zwłaszcza przez jednostki samorządu terytorialnego, z powołaniem się na ochronę danych,
- możliwość stosowania monitoringu wizyjnego, np. przez pracodawców,
- ujawnianie danych i wizerunku osób opisywanych przez media.

Tematy te pojawiały się już w latach ubiegłych, ale nasilenie niektórych wątków nastąpiło w związku z rozpoczęciem obowiązywania RODO. Jeśli chodzi zaś o treść RODO i działanie Urzędu Ochrony Danych Osobowych, dziennikarzy interesowało zwłaszcza:

- liczba skarg, pytań oraz zgłoszonych naruszeń,
- korzystanie przez Prezesa UODO z sankcji, w tym szczególnie nakładanie kar finansowych, wobec administratorów łamiących zasady ochrony danych osobowych,
- sposób reakcji Prezesa UODO na wycieki danych,
- przetwarzanie danych osobowych w związku z organizacją wyborów, w procesie rekrutacji, przez szkoły oraz placówki zdrowia,
- realizacja prawa do bycia zapomnianym.

2.4. Wywiady prasowe

W 2018 r. GIODO, a następnie Prezes UODO oraz eksperci GIODO/UODO udzielili ponad 100 wywiadów. Ich tematyka była różnorodna, choć dominowały zagadnienia dotyczące zasad ochrony danych osobowych, które wynikają z RODO oraz przepisów branżowych. Dziennikarzy interesowały takie zagadnienia, jak: skargi na administratorów, kategorie najczęściej zgłaszanych naruszeń, przebieg kontroli przestrzegania przepisów RODO, sposoby zapewnienia zgodności z RODO, sankcjeza niezgodne z prawem przetwarzanie danych osobowych, oceny stanu przygotowania różnych podmiotów do stosowania RODO.

Dziennikarze dopytywali także o kwestie bardziej złożone, np., jak chronić dane osobowe w kontakcie z telemarketerami, jak organizować zbiórkę podpisów pod akcją poparcia, czy tablice rejestracyjne można traktować jako dane osobowe, jak opracowywać kodeksy postępowania, jakie zadania realizuje IOD, jak zgodnie z RODO prowadzić rejestry publiczne lub znakować śmieci.

2.5. Spotkania prasowe

Prezes UODO systematycznie inicjował różnorakie spotkania z przedstawicielami mediów w związku z popularyzowaniem zadań realizowanych przez organ nadzorczy.

W 2018 r. odbyło się 12 takich spotkań (konferencji prasowych oraz briefingów). Były one poświęcone m.in.: podsumowaniu stanu przygotowania do rozpoczęcia stosowania RODO, monitoringowi wizyjnemu, przetwarzaniu danych przez pracodawców. Były one stałym elementem towarzyszącym upowszechnieniu informacji o XII Dniu Ochrony Danych Osobowych oraz VIII edycji programu edukacyjnego „Twoje dane – Twoja sprawa".

Spotkania prasowe były także inicjowane w związku z prezentacjami poradników poświęconych ochronie danych osobowych w szkole i placówkach oświatowych, w miejscu pracy oraz podczas wyborów.

2.6. Infolinia

12 marca 2018 r.- dwa i pół miesiąca przed początkiem stosowania RODO – uruchomiona została infolinia GIODO. Na początku funkcjonowania w infolinii pracowały trzy osoby, a od września 2018 r. – cztery. Planowane jest powiększenie składu zespołu infolinii.

Pracownicy infolinii posiadają wiedzę z zakresu ochrony danych osobowych, którą systematycznie podnoszą uczestnicząc w specjalistycznych szkoleniach oraz monitorując aktualny stan prawny w tym orzecznictwo krajowe i europejskie oraz wydane przez Prezesa UODO decyzje administracyjne.

W 2018 roku pytania zadawane przez osoby dzwoniące na infolinię koncentrowały się wokół kilku kwestii, w tym m.in. powtarzającego się pytania o możliwość zgodnego z prawem kopiowania (skanowania) dokumentów potwierdzających tożsamość. Z perspektywy czasu, z przeprowadzonych rozmów można wnioskować, że, m.in. dzięki uruchomieniu infolinii, zwiększyła się świadomość w zakresie udostępniania swojego dokumentu tożsamości. Zmniejszyła się także liczba podmiotów domagających się kopii dowodu osobistego (głównie firmy telekomunikacyjne).

Kolejnym problemem poruszanym przez interesantów były telefony, SMS-y czy maile z zakresu marketingu bezpośredniego (oferty sprzedażowe, zaproszenia na prezentacje produktu itp.). Bardzo często wykonywanie połączeń telefonicznych oraz przesyłanie wiadomości e-mail zawierających informacje handlowe odbywa się z naruszeniem przepisów prawa. Eksperci GIODO/UODO, udzielający odpowiedzi na związane z opisanym problemem pytania, podkreślali, że żeby móc wysłać e-mail z ofertą lub zadzwonić z propozycją zaproszenia na prezentację produktu trzeba najpierw uzyskać zgodę odpowiednio: na otrzymywanie informacji handlowych drogą elektroniczną oraz na wykonanie takiego połączenia telefonicznego w celach marketingowych. Wynika to z art. 10 Ustawy z 18 lipca 2002 r. o świadczeniu usług droga elektroniczną i art. 172 Ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne. Zasadniczo organami właściwymi w takich sprawach są Urząd Komunikacji Elektronicznej i Urząd Ochrony Konkurencji i Konsumentów. Można też kierować skargi do Prezesa UODO, ale niezbędne jest ustalenie danych podmiotu, który przetwarza dane osobowe w postaci numeru telefonu [212].

Dzwoniący na infolinię często skarżyli się również na uciążliwe telefony od firm windykacyjnych. Zasadniczo nie jest to jednak materia leżąca w kompetencji organu nadzorczego, do którego można kierować skargi na ujawnianie informacji o długu osobom nieuprawnionym.

Korzystający z infolinii pytali ekspertów o kierowane do nich żądania podania numeru PESEL, jako niezbędnego do zawarcia umowy, złożenia wniosku w urzędzie czy do weryfikacji w rozmaitych sytuacjach w celu uzyskania informacji przez telefon. Podawane w mediach informacje o wyłudzeniach kredytu z użyciem cudzych danych osobowych poskutkowały wzmożonym zainteresowaniem ochroną danych osobowych. UODO uznaje, że numer PESEL powinien być dobrze

[212] Wynika to z Kodeksu Postępowania Administracyjnego. Nasz Urząd nie może ustalić podmiotu po samym numerze telefonu, z którego wykonano połączenie, gdyż w stosunku do niego nie może być uchylona tajemnica telekomunikacyjna z urzędu.

chroniony i ujawniany tylko wtedy, gdy jest to konieczne, np. jeśli jest to niezbędne do jednoznacznej weryfikacji osoby.

Inne pytania zadawane ekspertom infolinii dotyczyły często samej istoty ochrony danych osobowych – czym są dane osobowe, kiedy ich przetwarzanie podlega przepisom prawa, czy w konkretnej sytuacji naruszono ochronę czyichś danych osobowych i co zrobić w takiej sytuacji. Ostatnie zagadnienie związane jest z ujawnianiem danych osobowych osobom nieuprawnionym. Dochodzi do tego np. w sytuacji dopuszczenia do przetwarzania danych osobowych przez osoby nieupoważnione, czy skierowania przesyłki do innego adresata albo zaginięcia przesyłki oznaczonej danymi osobowymi.

Wśród pytań kierowanych do ekspertów UODO znalazły się kwestie związane z oszustwami lub próbami wyłudzeń. Często opisywano próby wyłudzeń związane ze szkoleniami/audytami z zakresu ochrony danych osobowych, polegające np. na kierowaniu do przedsiębiorców oferty szkoleniowa z zakresu RODO, sugerująca,, że udział w szkoleniu pozwoli uniknąć kar nakładanych przez UODO lub oferta przeprowadzenia audytu z informacją, że o jego nieprzeprowadzeniu przez firmę zostanie poinformowany Prezes UODO. Pracownicy infolinii zawsze informowali dzwoniących o ich rzeczywistych obowiązkach, wynikających z RODO, sami przeprowadzali telefonicznie krótkie szkolenie w podstawowym zakresie, a o próbach wyłudzeń informowano Policję[213].

Pytania kierowane od przedsiębiorców i podmiotów publicznych często powtarzały się i dotyczyły podstawowych wymogów wskazanych w RODO. Pytania dotyczyły najczęściej treści klauzuli informacyjnej i sposobów jej komunikowania osobom, których dane są przetwarzane. Poza tym pytania dotyczyły rejestrów prowadzonych na mocy art. 30 RODO[214], rozpoznania, czy mamy do czynienia z udostępnieniem danych innemu administratorowi czy z ich powierzeniem - do czego potrzebne jest zawarcie umowy powierzenia zgodnie z art. 28 RODO.

Zarówno przedsiębiorcy, jak i podmioty publiczne wskazywały też na problemy związane z transferem danych do państw trzecich (poza Europejski Obszar Gospodarczy). Pracownicy infolinii najczęściej rozpoznawali sytuację i wskazywali możliwości zgodnego z prawem transferu danych. Jeśli opisywany przez dzwoniącego stan faktyczny był szczególnie skomplikowany, proszono o przesłanie pytania pisemnie lub elektronicznie.

Do wspólnego zakresu pytań zadawanych zarówno przez podmioty prywatne, jak i publiczne, należy zaliczyć także te o obowiązek (i jego zakres) udostępniania danych instytucjom publicznym (komornicy, organy ścigania, urzędy skarbowe, ośrodki pomocy społecznej). UODO stoi na stanowisku, że do takiego udostępnienia musi istnieć podstawa wskazana w przepisach prawa.

Do pytań kierowanych tylko z instytucji publicznych należą kwestie dostępu do informacji publicznej na jej styku z ochroną prywatności urzędników i osób fizycznych. Eksperci UODO w miarę możliwości starali się odpowiedzieć na pytanie, mimo że zasadniczo nie jest to kwestia ochrony danych osobowych a stosowania Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz.U. 2001 nr 112 poz. 1198, ze zm.

Z rozmów przeprowadzanych na infolinii wynika jednoznacznie, że Polacy cenią swoją prywatność i starają się ja chronić na różne sposoby, także angażując w to Urząd Ochrony Danych Osobowych.

Warto podkreślić, że trzyosobowy skład infolinii odbierał średnio 90 telefonów dziennie, a cztery osoby odbierały łącznie ok. 115 połączeń każdego dnia.

[213] W tym celu Prezes UODO wyznaczył jednego z pracowników infolinii, który składał na Policji odpowiednie zawiadomienia.

[214] Urząd wydał wskazówki jak je prowadzić: https://uodo.gov.pl/pl/383/214.

2.7. Telefoniczne dyżury eksperckie

Upowszechnianiu informacji na temat zasad ochrony danych osobowych służyły też telefoniczne dyżury eksperckie, organizowane we współpracy z mediami. Miały one na celu przede wszystkim przybliżenie nowych, określonych w RODO zasad przetwarzania danych osobowych oraz praw, jakie na mocy tego aktu prawnego przysługują każdemu z nas. Przykładem takich dyżurów były spotkania zorganizowane 26 lutego 2018 r. we współpracy z portalem Infor.pl oraz 30 stycznia 2018 r. – dyżur w regionalnej rozgłośni Polskiego Radia w Łodzi.

2.8. Akcje informacyjno-edukacyjne

W 2018 r. realizowano wiele dodatkowych działań upowszechniających działalność najpierw GIODO, a potem Prezesa UODO, w tym zwłaszcza prowadzonych w związku z RODO.

Przykładem akcji informacyjno-edukacyjnych jest m.in.: specjalne spotkanie z dziennikarzami zorganizowane tuż przed 25 maja 2018 r., podczas którego Generalny Inspektor Ochrony Danych Osobowych wraz z dyrektorami przedstawił stan przygotowania do rozpoczęcia stosowania RODO. Z kolei, po upływie sześciu miesięcy od tego wydarzenia, przygotowano dwa opracowania tematyczne, które za pośrednictwem mediów trafiły do opinii publicznej: „10 wskazówek, jak korzystać z praw gwarantowanych przez RODO" oraz „10 wskazówek dla administratorów, jak stosować RODO".

Innym przykładem akcji informacyjnych jest coroczna akcja koordynowana przez UOKiK „Przed wakacjami – co warto wiedzieć". W 2018 r. organ nadzorczy przygotował na potrzeby tej akcji tekst pt. „Jak korzystać z aplikacji, by nasz telefon lub smartwatch był pomocnym przyjacielem, a nie szpiegiem", który dodatkowo był dostępny dla opinii publicznej za pośrednictwem strony www.uodo.gov.pl. Opublikowały go na swoich stronach internetowych także 52 pozostałe instytucje, biorące udział w tym przedsięwzięciu.

IV. UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ PROBLEMATYKĄ OCHRONY DANYCH OSOBOWYCH

Jednym z ustawowych zadań organu właściwego w sprawach ochrony danych osobowych jest uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. Zadanie to realizowane było przede wszystkim poprzez udział GIODO/Prezesa UODO 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 GIODO/Prezesa UODO prowadzonych w ramach współpracy międzynarodowej w okresie sprawozdawczym należał udział w posiedzeniach Grupy Roboczej Art. 29 ds. Ochrony Danych, którą 25 maja 2018 r. zastąpiła Europejska Rada Ochrony Danych, w tym w pracach jej podgrup eksperckich. GIODO/Prezes UODO brał także udział w pracach Komitetu Konsultacyjnego Rady Europy, współpracował 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 brał 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, IMI, Eurodac, Wspólnego Organu Nadzorczego nad Systemem Informacji Celnej (CIS), Rady Współpracy Europolu, a także Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupy Berlińskiej).

1. Grupa Robocza Art. 29

W omawianym roku sprawozdawczym 2018 r., w okresie przed rozpoczęciem stosowania RODO, GIODO uczestniczył w cyklicznie odbywających się spotkaniach Grupy Roboczej Art. 29 ds. Ochrony Danych (GR Art. 29) organizowanych w Brukseli. GR Art. 29 ustanowiona została na podstawie art. 29 dyrektywy 95/46/WE, w jej skład wchodzili przedstawiciele każdego państwa członkowskiego UE, Europejski Inspektor Ochrony Danych Osobowych oraz przedstawiciel Komisji Europejskiej.

Do zadań GR Art. 29 należało badanie wszelkich kwestii dotyczących stosowania krajowych środków przyjętych na mocy ww. dyrektywy (w celu jednolitego stosowania tych środków), przekazywanie Komisji Europejskiej opinii na temat stopnia ochrony prywatności i danych osobowych w UE 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 miały zastosowanie również w odniesieniu do sektora łączności elektronicznej.

W roku 2018 Grupa Robocza Art. 29 kontynuowała prace nad opracowaniem bądź zmianą kluczowych dokumentów dotyczących interpretacji i wdrażania RODO. Wśród przyjętych dokumentów znalazły się:

- (zmienione) Wytyczne dotyczące zgłoszeń naruszeń ochrony danych zgodnie z Rozporządzeniem 2016/679 (WP250 rev.01);
- (zmienione) Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidulanych przypadkach i profilowania do celów Rozporządzenia 2016/679 (WP251 rev.01);
- (zmienione) Wytyczne dotyczące zgody na mocy Rozporządzenia 2016/679 (WP259 rev.01);
- (zmienione) Wytyczne dotyczące przejrzystości na podstawie Rozporządzenia 2016/679 (WP260 rev.01);
- Projekt wytycznych w sprawie akredytacji podmiotów certyfikujących na podstawie Rozporządzenia 2016/679 (WP261),które miały być poddane publicznym konsultacjom;
- Wytyczne dotyczące artykułu 49 Rozporządzenia 2016/679 (WP262), które miały być poddane publicznym konsultacjom.

GR Art. 29 przyjęła również Opinię dotyczącą wniosków Komisji w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze granic i wiz oraz współpracy policyjnej i sądowej, azylu i migracji (WP266).

GR Art. 29 prowadziła także prace nad organizacją i strukturą Europejskiej Rady Ochrony Danych (EROD), która wraz z rozpoczęciem stosowania RODO 25 maja 2018 r. zastąpiła Grupę Roboczą Art. 29.

Udział GIODO i jego przedstawicieli w pracach Grupy Roboczej Art. 29 ds. Ochrony Danych należy uznać za niezwykle istotny, bowiem działania prowadzone w ramach GR Art. 29 stanowiły wyznacznik działań europejskich organów ochrony danych, w tym polskiego organu.

Posiedzenia Grupy Roboczej Art. 29:

- **114. posiedzenie Grupy Roboczej Artykułu 29**

Przedstawiciel GIODO uczestniczył 6–7 lutego 2018 r. w 114. posiedzeniu Grupy Roboczej Artykułu 29 ds. Ochrony Danych w Brukseli, podczas którego przeanalizowano istotne kwestie dotyczące wdrożenia RODO, a także przyjęto siedem kluczowych dokumentów na potrzeby przygotowania do stosowania RODO od 25 maja 2018 r.

- **115. posiedzenie Grupy Roboczej Artykułu 29**

Podczas 115. posiedzenia GR Art. 29, które odbyło się 10–11 kwietnia 2018 r. z udziałem GIODO, dodatkowo przyjęto szereg kluczowych dokumentów na potrzeby przygotowania do stosowania RODO od 25 maja 2018 r., np. wytyczne dotyczące zgody i przejrzystości, oraz ustanowiono Grupę Roboczą ds. Mediów Społecznościowych w świetle ostatnich doniesień dotyczących Facebooka /Cambridge Analytica.

2. Europejska Rada Ochrony Danych (EROD)

Od 25 maja 2018 r. Europejska Rada Ochrony Danych zastąpiła Grupę Roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołaną na mocy art. 29 Dyrektywy 95/46/WE. EROD została ustanowiona na mocy art. 68 ust. 1 **RODO.**

EROD, jako organ Unii Europejskiej, posiada osobowość prawną. W skład Rady wchodzą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych (**EIOD**) lub ich przedstawiciele. Komisja Europejska ma prawo udziału w działaniach i posiedzeniach EROD, nie ma jednak prawa głosu. Radę reprezentuje jej przewodniczący.

EROD w toku wypełniania swoich zadań lub wykonywania swoich uprawnień na mocy art. 70 i 71 RODO działa w sposób niezależny.

EROD ma na celu zapewnienie spójnego stosowania RODO w całej Unii Europejskiej, jak również spójnej ochrony danych osób fizycznych. Posiada również dodatkowe kompetencje, m.in.: doradza Komisji Europejskiej, promuje współpracę pomiędzy krajowymi organami nadzorczymi oraz odgrywa istotną rolę w procedurach pojednawczych w przypadku sporów między krajowymi organami ochrony danych. Wykonując swoje uprawnienia, EROD wydaje wytyczne, zalecenia i oświadczenia dotyczące najlepszych praktyk.

Prezes UODO lub jego przedstawiciel uczestniczyli w odbywających się co miesiąc w Brukseli posiedzeniach plenarnych EROD. **Pierwsze posiedzenie plenarne EROD odbyło się 25 maja 2018 r.**

Podczas pierwszego posiedzenia EROD wybrała na najbliższe pięć lat przewodniczącego oraz dwóch wiceprzewodniczących. Zatwierdzono również następujące dokumenty wydane przez Grupę Roboczą Art. 29, tj.:

1) Wytyczne dotyczące zgłoszeń naruszeń ochrony danych zgodnie z Rozporządzeniem 2016/679 (WP250 rev.01);
2) Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidulanych przypadkach i profilowania do celów Rozporządzenia 2016/679 (WP251 rev.01);
3) Wytyczne dotyczące zgody na mocy Rozporządzenia 2016/679 (WP259 rev.01);
4) Wytyczne dotyczące przejrzystości na podstawie Rozporządzenia 2016/679 (WP260 rev.01);
5) Dokument dotyczący adekwatności (WP 254);
6) Dokument Roboczy Dotyczący Wiążących Reguł Korporacyjnych dla Przetwarzających (WP 257);
7) Dokument Roboczy Dotyczący Wiążących Reguł Korporacyjnych dla Administratorów (WP 256);
8) Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów Rozporządzenia nr 2016/679 (WP 253);
9) Wytyczne dotyczące prawa do przenoszenia danych (WP242 rev.01);

10) Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów Rozporządzenia 2016/679 (WP248 rev. 01);
11) Wytyczne dotyczące inspektorów ochrony danych („DPO") (WP243 rev.01);
12) Wytyczne dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP244 rev.01);
13) Zalecenie dot. standardowego wniosku o zatwierdzenie Wiążących Reguł Korporacyjnych dla administratora danych dla celów przekazywania danych osobowych (WP264);
14) Zalecenie dot. standardowego wniosku o zatwierdzenie Wiążących Reguł Korporacyjnych dla podmiotów przetwarzających dla celów przekazywania danych osobowych (WP265);
15) Dokument Roboczy ustanawiający procedurę współpracy w celu zatwierdzenia „wiążących reguł korporacyjnych" dla administratorów i podmiotów przetwarzających zgodnie z RODO (WP263 rev.01);
16) Stanowisko w sprawie odstępstw od obowiązku prowadzenia rejestru czynności przetwarzania danych osobowych zgodnie z art. 30 ust. 5 RODO.

Podczas pierwszego posiedzenia plenarnego, EROD przyjęła pierwsze wytyczne, tj.: 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 Rozporządzenia 2016/679 oraz Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 Rozporządzenia 2016/679.

Drugie posiedzenie plenarne EROD odbyło się 4–5 lipca 2018 r.

Podczas posiedzenia poruszono m.in. następujące kwestie:

- Procedury współpracy i spójności – aktualna sytuacja

EROD omówiła mechanizm spójności i mechanizm współpracy, dzieląc się doświadczeniem w zakresie funkcjonowania mechanizmu kompleksowej współpracy oraz działania systemu wymiany informacji na rynku wewnętrznym (IMI), który stanowi platformę informatyczną służącą do wymiany informacji na temat spraw o charakterze transgranicznym. EROD odniosła się także do wyzwań, przed jakimi stoją organy ochrony danych, a także do rodzaju pytań napływających od 25 maja 2018 r. Większość organów ochrony danych odnotowała znaczny wzrost liczby składanych skarg. Pierwsze sprawy wprowadzono do IMI w dniu 25 maja.

- Internetowa Korporacja ds. Nadawania Nazw i Numerów

EROD przyjęła w imieniu jej przewodniczącej pismo skierowane do Internetowej Korporacji ds. Nadawania Nazw i Numerów (ICANN), w którym zawarto wytyczne umożliwiające ICANN opracowanie zgodnego z RODO modelu wniosku o dostęp do danych osobowych przetwarzanych w kontekście bazy danych WHOIS. W piśmie tym poruszono takie kwestie jak określenie celu, gromadzenie „pełnych danych WHOIS", rejestracja osób prawnych, rejestrowanie dostępu do niepublicznych danych WHOIS, zatrzymywanie danych oraz kodeksy postępowania i akredytacja. Od 2003 r. Grupa Robocza Art. 29, opracowywała dla ICANN wytyczne dotyczące tego, jak zapewnić zgodność WHOIS z przepisami UE w zakresie ochrony danych. EROD oczekuje, że ICANN opracuje i wdroży model WHOIS, który umożliwi właściwym zainteresowanym podmiotom takim jak organy ds. egzekwowania prawa, zgodne z prawem wykorzystywanie danych osobowych dotyczących rejestrujących zgodnie z ogólnym rozporządzeniem o ochronie danych, tak aby nie prowadziło to do publikacji takich danych na nieograniczoną skalę.

- Druga dyrektywa w sprawie usług płatniczych

EROD przyjęła w imieniu jej przewodniczącej pismo skierowane do Sophie in't Veld, posłanki do Parlamentu Europejskiego, dotyczące zmienionej drugiej dyrektywy w sprawie usług płatniczych. W odpowiedzi skierowanej do Sophie in't Veld EROD rzuca więcej światła na kwestię danych milczącej strony (ang. silent party), dostarczanych przez dostawców będących stronami trzecimi, na procedury dotyczące wyrażenia i wycofania zgody, regulacyjne standardy techniczne, współpracę między

bankami i Komisją Europejską, EIOD i Grupą Roboczą Art. 29 oraz na to, co jeszcze należy zrobić, by wyeliminować wszelkie pozostałe luki w ochronie danych.

- Tarcza Prywatności

Ambasador Judith Garber, Rzecznik ds. Tarczy Prywatności w USA odpowiedzialna za rozpatrywanie skarg dotyczących bezpieczeństwa narodowego w ramach Tarczy Prywatności, została zaproszona do udziału w dyskusji z członkami EROD na posiedzeniu plenarnym. Członkowie EROD byli szczególnie zainteresowani kwestiami budzącymi niepokój zgłaszanymi USA przez Grupę Roboczą Art. 29. Mowa tu przede wszystkim o kwestii mianowania stałego Rzecznika, formalnego mianowania członków do Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (PCLOB) i braku dodatkowych informacji na temat mechanizmu Rzecznika ds. Tarczy Prywatności i dalszego zniesienia klauzuli tajności, którą opatrzone są przepisy proceduralne, zwłaszcza te dotyczące kontaktów Rzecznika ze służbami wywiadu.

EROD podkreśliła, że spotkanie z Rzecznikiem ds. Tarczy Prywatności było interesujące i przebiegało w przyjaznej atmosferze, lecz nie przyniosło rozstrzygającej odpowiedzi na wspomniane wyżej kwestie i że kwestie te pozostaną w centrum uwagi w trakcie drugiego rocznego przeglądu (zaplanowanego na październik 2018 r.). Ponadto EROD wezwała władze USA do przedłożenia dodatkowych dowodów, aby rozwiązać omawiane kwestie. EROD zwróciła także uwagę, że te same kwestie zostaną poruszone przez Trybunał Sprawiedliwości w sprawach, które już się toczą i w ramach których EROD chętnie zabierze głos na prośbę Trybunał Sprawiedliwości.

Trzecie posiedzenie plenarne odbyło się 25–26 września 2018 r.

Poruszono na nim m.in. następujące kwestie:

- Unijna decyzja stwierdzająca odpowiedni stopień ochrony w Japonii

Członkowie EROD omówili projekt unijnej decyzji stwierdzającej odpowiedni stopień ochrony w Japonii, który przekazała im Komisarz Věra Jourová z prośbą o przedstawienie opinii w tej kwestii. EROD zapowiedziała dokonanie gruntownego przeglądu projektu decyzji. EROD zaplanowała wzięcie pod uwagę daleko idących skutków projektu decyzji, jak również potrzeby ochrony danych osobowych w UE.

- Wykazy rodzajów operacji przetwarzania wymagających oceny skutków dla ochrony danych

EROD przyjęła 22 opinie ustanawiające wspólne kryteria dla wykazów rodzajów operacji przetwarzania wymagających oceny skutków dla ochrony danych. Wykazy te stanowią ważne narzędzie do spójnego stosowania RODO w całej UE. Ocena skutków dla ochrony danych to proces ułatwiający identyfikację i minimalizowanie ryzyka związanego z ochroną danych, które może wpłynąć na prawa i wolności osób fizycznych. Żeby pomóc w wyjaśnieniu rodzajów przetwarzania, które mogą wymagać oceny skutków dla ochrony danych, RODO wzywa krajowe organy nadzorcze do tworzenia i publikowania wykazów rodzajów operacji, które mogą wiązać się z wysokim ryzykiem. EROD otrzymała 22 krajowe wykazy zawierające różne rodzaje przetwarzania w łącznej liczbie 260. Dwadzieścia dwie opinie na temat wykazów rodzajów operacji przetwarzania wymagających oceny skutków dla ochrony danych wynikają z art. 35 ust. 4 i art. 35 ust. 6 RODO i są zgodne z wcześniejszymi wytycznymi ustanowionymi przez Grupę Roboczą Art. 29.

- Wytyczne dotyczące zakresu terytorialnego

EROD przyjęła nowy projekt wytycznych, które pomogą w zapewnieniu wspólnych interpretacji dotyczących zakresu terytorialnego RODO. Zapewnią one dalsze wyjaśnienia dotyczące stosowania RODO w różnych sytuacjach, w szczególności w przypadku, gdy administrator albo podmiot przetwarzający ma siedzibę poza UE, w tym w sprawie wyznaczenia przedstawiciela. Wytyczne zostały oddane do konsultacji społecznych.

- Elektroniczne materiały dowodowe

EROD przyjęła opinię dotyczącą regulacji w zakresie elektronicznych materiałów dowodowych, która została zaproponowana przez Komisję Europejską w kwietniu 2018 r. EROD podkreśliła, że proponowane nowe zasady dotyczące gromadzenia elektronicznych materiałów dowodowych

powinny w wystarczającym stopniu chronić prawa osób fizycznych do ochrony danych i powinny być bardziej spójne z unijnymi przepisami dotyczącymi ochrony danych.

Czwarte posiedzenie plenarne odbyło się 16 listopada 2018 r.

Poruszono na nim następujące kwestie:

- Projekt decyzji stwierdzającej odpowiedni stopień ochrony danych w Japonii
- Członkowie EROD omówili stan prac nad projektem decyzji stwierdzającej odpowiedni stopień ochrony danych w Japonii, który EROD otrzymała od komisarz Věry Jourovej we wrześniu 2018 r. EROD ponownie podkreśliła znaczenie zagwarantowania ciągłości i wysokiego poziomu ochrony przekazywania danych z UE.
- Rozporządzenie w sprawie badań klinicznych

EROD udziela wskazówek w zakresie pytań i odpowiedzi na temat badań klinicznych w kontekście wzajemnych zależności między RODO, a rozporządzeniem w sprawie badań klinicznych. Po konsultacjach z Komisją Europejską EROD uzgodniła przyznanie mandatu w zakresie opracowania wytycznych w sprawie pytań i odpowiedzi, opracowanych przez Komisję, dotyczących wzajemnych zależności między RODO, a rozporządzeniem w sprawie badań klinicznych.

- Wytyczne dotyczące terytorialnego zakresu stosowania

Podczas wrześniowej sesji plenarnej EROD przyjęła nowe projekty wytycznych, które pomogą w osiągnięciu spójnej interpretacji terytorialnego zakresu stosowania RODO oraz pozwolą na doprecyzowanie kwestii związanych ze stosowaniem rozporządzenia w różnych sytuacjach, w szczególności gdy administrator lub podmiot przetwarzający dane mają siedzibę poza UE. Jedną z takich kwestii jest wyznaczanie przedstawiciela. Jako że standardowe końcowe kontrole prawne przeprowadzone przed publikacją ujawniły, że niektóre kwestie wymagają dalszej dyskusji, EROD postanowiła ponownie omówić te wytyczne podczas listopadowej sesji plenarnej. Kwestie te zostały omówione i uzgodnione, a wytyczne miały zostać wkrótce opublikowane i skierowane do konsultacji publicznych.

Piąte posiedzenie plenarne odbyło się 4–5 grudnia 2018 r.

Poruszono na nim m.in. następujące kwestie:

- Projekt decyzji stwierdzającej odpowiedni stopień ochrony danych osobowych w Japonii

Członkowie EROD przyjęli opinię w sprawie projektu decyzji stwierdzającej odpowiedni stopień ochrony danych osobowych w Japonii, który został przekazany Radzie przez Komisję Europejską we wrześniu 2018 r. EROD dokonała oceny na podstawie dokumentacji udostępnionej przez Komisję Europejską. Najważniejszym celem EROD było sprawdzenie, czy japońskie przepisy ramowe zapewniają odpowiedni stopień ochrony danych osobowych osób fizycznych. Należy przy tym pamiętać o tym, że EROD nie oczekiwała, że japońskie ramy prawne będą powielać europejskie przepisy o ochronie danych. EROD z zadowoleniem przyjęła starania podjęte przez Komisję Europejską i Japońską Komisję Ochrony Danych (PPC) na rzecz zwiększenia konwergencji japońskich i europejskich ram prawnych. Poprawki wprowadzone w przepisach uzupełniających, których celem jest zniwelowanie pewnych różnic między tymi dwoma systemami, są bardzo ważne i spotkały się z pozytywnym przyjęciem. Jednak w następstwie dokładnej analizy projektu decyzji Komisji stwierdzającej odpowiedni stopień ochrony danych w Japonii, a także analizy obowiązujących w Japonii ramowych przepisów o ochronie danych, EROD zauważyła, że nadal istnieje szereg problemów, takich jak ochrona przekazywanych z UE do Japonii danych osobowych – w ciągu całego cyklu ich życia. EROD zaleciła również Komisji Europejskiej rozpatrzenie złożonych przez EROD wniosków o wyjaśnienia, przedstawienie dalszych dowodów i wyjaśnień dotyczących podniesionych kwestii, a także ścisłe monitorowanie skuteczności stosowania przyjętych rozwiązań.

Zdaniem EROD decyzja stwierdzająca odpowiedni stopień ochrony danych w Japonii ma ogromne znaczenie i stanowi precedens – będąc pierwszą decyzja stwierdzająca odpowiedni stopień ochrony danych od momentu wejścia w życie RODO.

- Wykazy rodzajów operacji przetwarzania wymagających oceny skutków dla ochrony danych

EROD przyjęła opinie w sprawie wykazów operacji przetwarzania wymagających oceny skutków dla ochrony danych przekazanych przez Danię, Chorwację, Luksemburg i Słowenię. Wspomniane wykazy stanowią ważne narzędzie służące spójnemu stosowaniu RODO w całym EOG. Ocena skutków dla ochrony danych to proces pomocny w identyfikowaniu i ograniczaniu zagrożeń związanych z ochroną danych, które mogą mieć wpływ na prawa i wolności osób fizycznych. Rozważenie, czy przed podjęciem działalności związanej z przetwarzaniem niezbędne jest dokonanie oceny skutków dla ochrony danych, należy zasadniczo do obowiązków administratora. Krajowe organy nadzorcze są natomiast odpowiedzialne za sporządzenie i opublikowanie wykazu rodzajów operacji przetwarzania, które podlegają wymogowi przeprowadzenia oceny skutków dla ochrony danych.

Cztery wymienione opinie, wraz z 22 przyjętymi już podczas posiedzenia wrześniowego, przyczynią się do ustanowienia wspólnych kryteriów dla wykazów operacji przetwarzania wymagających oceny skutków dla ochrony danych na terytorium EOG.

- Wytyczne w sprawie akredytacji

EROD przyjęła zmienioną wersję wytycznych w sprawie akredytacji przygotowanych przez Grupę Roboczą Art. 29, w tym nowy załącznik do wytycznych. Projekt wytycznych został pierwotnie przyjęty przez Grupę Roboczą Art. 29, a następnie przekazany do konsultacji publicznych. EROD zakończyła analizę i osiągnęła porozumienie w sprawie ostatecznej wersji. Celem wytycznych jest udostępnienie wskazówek dotyczących interpretowania i wdrożenia przepisów art. 43 RODO. Przede wszystkim mają one pomóc państwom członkowskim, organom nadzorczym i krajowym jednostkom akredytującym w ustanowieniu spójnej i ujednoliconej podstawy na potrzeby akredytowania jednostek certyfikujących, które wydają certyfikaty zgodnie z RODO. Wytyczne zostały uzupełnione o załącznik, w którym znajdują się wskazówki odnośnie do dodatkowych wymogów w zakresie akredytowania jednostek certyfikujących, które to wymogi powinny zostać wprowadzone przez organy nadzorcze. Załącznik miał być przedmiotem konsultacji publicznych.

Udział Prezesa UODO w posiedzeniach plenarnych EROD miało kluczowe znaczenie nie tylko z punktu widzenia przestrzegania mechanizmu spójności i współpracy, o którym mowa w rozdziale VII RODO, ale również, jak potwierdza doświadczenie pierwszego roku stosowania RODO, z punktu widzenia wypracowywania spójnych z europejskimi wytycznymi stanowisk, a w konsekwencji ujednolicenia praktyki orzeczniczej UODO.

Mając na uwadze powyższe oraz fakt, że zgodnie z RODO, udział w pracach EROD stanowi obowiązek każdego organu nadzorczego, uczestnictwo Prezesa UODO w posiedzeniach plenarnych EROD uznać należy za niezwykle istotne.

3. Działalność podgrup eksperckich EROD

Zgodnie z art. 25 Regulaminu Europejskiej Rady Ochrony Danych (EROD), działa ona poprzez wewnętrzne podgrupy eksperckie, które wspierają Radę w wykonywaniu jej zadań. W spotkaniach podgrup Rady uczestniczą przedstawiciele organów nadzorczych Państw Członkowskich UE, w tym przedstawiciele UODO.

W skład EROD w 2018 roku wchodziły następujące podgrupy: Technology, Cooperation, BTLE – Boarders, Travel & Law Enforcement, Key Provisions, Fining Taskforce, Future Of Privacy, e-Government, Social Media, IT Users, International Transfers, Financial Matters oraz Enforcement,

W okresie sprawozdawczym przedstawiciele UODO uczestniczyli m.in. w następujących spotkaniach:

- 4–5.09.2018 r. – spotkanie podgrupy Technology, której zadaniem była analiza wykazów operacji przetwarzania.
- 5.09.2018 r. – spotkanie podgrupy Cooperation, kompetentnej w zakresie współpracy między organami ochrony danych. Podczas spotkania członkowie podgrupy dyskutowali nad interpretacją art. 64 ust. 2 RODO, umożliwiającego m.in. organom nadzorczym występowanie do Rady o przeanalizowanie sprawy w celu wydania opinii.

- 6.09.2018 r. odbyło się spotkanie podgrupy BTLE – Boarders, Travel & Law Enforcement, zajmującej się sprawami związanymi z bezpieczeństwem danych przekazywanych do państw trzecich i transgranicznym przetwarzaniem danych. Grupa podczas spotkania pracowała m.in. nad wytycznymi do art. 48 RODO, wskazującego tryb przekazywania lub ujawniania danych państwu trzeciemu.
- 7.09.2018 r. – spotkanie podgrupy Key Provisions, zajmującej się stosowaniem kluczowych postanowień RODO. Podczas spotkania podgrupa zajęła się kwestią stosowania art. 3 RODO wskazującego zakres terytorialny rozporządzenia, a także art. 6 ust. 1 lit. b RODO, czyli zagadnieniem jednej z przesłanek przetwarzania danych, jaką jest wykonanie umowy, w kontekście usług online.
- 7.09.2018 r. – spotkanie podgrupy Fining Taskforce, właściwej w zakresie stosowania nowego mechanizmu kar finansowych i ujednolicenia systemu kar.
- 11.09.2018 r. – spotkanie podgrupy Future Of Privacy, zajmującej się opracowywaniem strategii działań Rady. Podczas spotkania uczestnicy podjęli dyskusję m.in. nad priorytetami Rady w zakresie stosowania RODO, a także omówili kwestie przyszłej organizacji podgrup Rady.
- 13.09.2018 r. – spotkanie podgrupy e-Government, zajmującej się zagadnieniami związanymi między innymi z kodeksami postępowania. Grupa podczas spotkania pracowała będzie m.in. nad wytycznymi do art. 40 i 41 RODO, dotyczącymi kodeksów postępowania.
- 14.09.2018 r. – spotkanie podgrupy Social Media, kompetentnej w zakresie zagadnień związanych z ochroną prywatności w mediach społecznościowych. Uczestnicy spotkania podjęli dyskusję m.in. na temat nadzoru nad Facebookiem i związanymi z nim administratorami i podmiotami przetwarzającymi.
- 11.10.2018 r. – spotkanie podgrupy IT Users, zajmującej się zagadnieniami związanymi z systemem wymiany informacji na rynku wewnętrznym (system IMI). Podczas spotkania uczestnicy podjęli dyskusję dotyczącą rozwoju i ulepszania systemu IMI, a także innych narzędzi IT, które mogą być wykorzystywane w pracach Rady, takich jak np. system wideokonferencyjny.
- 16–17.10.2018 r. – spotkanie podgrupy International Transfers zajmującej się międzynarodowym transferem danych. Uczestnicy spotkania omawiali m.in. wytyczne do art. 46 RODO, decyzję stwierdzającą odpowiedni stopień ochrony zapewnianej przez Japonię oraz kwestie związane z wiążącymi regułami korporacyjnymi.
- 18.10.2018 r. – spotkanie podgrupy e-Government, podczas którego omówione zostały tematy związane z procedurą akceptacji kodeksów postępowania, wytycznymi do art. 40 i 41 RODO oraz podjęta została dyskusja nad dalszymi pracami podgrupy. .
- 30.10.2018 r. – spotkanie podgrupy BTLE – Boarders, Travel & Law Enforcement subgroup. Członkowie podgrupy podjęli dyskusję na tematy związane m.in. z decyzją stwierdzającą odpowiedni stopień ochrony zapewnianej przez Japonię, a także kwestiami dotyczącymi Tarczy Prywatności i kontroli nad danymi o przelocie pasażera (PNR).
- 6–7.11.2018 r. – spotkanie podgrupy Technology. Przedmiotem dyskusji grupy było wiele zagadnień z zakresu technologii, takich jak m.in.: analiza wykazów operacji przetwarzania wymagających oceny skutków dla ochrony danych, kwestie związane z monitoringiem wizyjnym, ochrona danych w fazie projektowania i domyślna (privacy by design and by default), certyfikacja i akredytacja.
- 8.11.2018 r. – spotkanie podgrupy Key Provisions. Uczestnicy spotkania pracowali nad dokumentem dotyczącym stosowania art. 6 ust. 1 lit. b RODO w kontekście świadczenia usług online.
- 9.11.2018 r. – spotkanie podgrupy Social Media, podczas którego podjęto dyskusję m.in. nad targetowaniem użytkowników Facebooka oraz planem działań podgrupy na 2019 r.
- 12.11.2018 r. – spotkanie grupy Enforcement, zajmującej się zagadnieniami egzekwowania prawa. Uczestnicy spotkania wymienili doświadczenia dotyczące egzekwowania prawa w reprezentowanych przez nich państwach członkowskich oraz przedyskutowali m.in. kwestie głównej siedziby i mechanizmu kompleksowej współpracy (one-stop-shop).
- 13–14.11.2018 r. – spotkanie grupy Cooperation, podczas którego podjęto dyskusję nad wytycznymi dotyczącymi procedur wynikających z art. 64 ust. 2 i 4 RODO, narzędziami dla ustalania wiodącego

organu nadzorczego (LSA), a także zagadnieniami związanymi ze współpracą międzynarodową w zw. z art. 50 RODO.

- 15.11.2018 r. – spotkanie grupy Fining Taskforce, podczas którego pracowano nad matrycą służącą do obliczania kar finansowych nakładanych przez organy nadzorcze na podstawie postanowień RODO.
- 19–20.11.2018 r. – spotkanie podgrupy e-Government. Uczestnicy spotkania rozmawiali m.in. nad wytycznymi do art. 40 and 41 RODO, dotyczącymi kodeksów postępowania, a także nad wytycznymi dotyczącymi ochrony danych w fazie projektowania i domyślnej.
- 11–12.12.2018 r. – spotkanie podgrupy International Transfers. Uczestnicy spotkania pracowali m.in. nad relacją pomiędzy art. 3, a rozdziałem V RODO, zagadnieniami związanymi z drugim rocznym przeglądem Tarczy Prywatności, wytycznymi do art. 46 RODO oraz wiążącymi regułami korporacyjnymi i standardowymi klauzami umownymi.
- 18.12.2018 r. odbyło się spotkanie podgrupy BTLE, podczas którego uczestnicy zajmowali się przede wszystkim zagadnieniami związanymi z drugim rocznym przeglądem Tarczy Prywatności, a także omawiali kwestie związane m.in. z rozporządzeniem e-Evidence i tzw. dyrektywą policyjną.
- 19.12.2018 r. spotkanie podgrupy Technology, podczas którego analizowano odpowiedzi na opinie EROD na temat przedstawionych przez organy nadzorcze list operacji wymagających oceny skutków dla ochrony danych (list DPIA). Podczas spotkania odbyła się również dyskusja na temat relacji pomiędzy dyrektywą ePrivacy a RODO.

4. Wizyty robocze

Wizyta Prezesa UODO w siedzibie gruzińskiego organu ochrony danych, Tbilisi (Gruzja), 12–17.11.2018 r.

Prezes UODO przebywał 12–17 listopada 2018 r. z wizytą w Urzędzie Inspektora Ochrony Danych Osobowych Gruzji w Tbilisi. Wśród zagadnień będących przedmiotem dyskusji podczas tego spotkania znalazły się m.in. kwestie związane z projektami realizowanymi w Gruzji w ramach Programu Rozwoju ONZ „Prawa człowieka dla wszystkich" oraz „Ułatwienie dostępu do wymiaru sprawiedliwości w Gruzji", wspieranego i finansowanego przez Unię Europejską.

5. Międzynarodowe Warsztaty

Warsztaty rozpatrywania spraw, Budapeszt (Węgry), 27–29.11.2018 r.

W Budapeszcie 27–29 listopada 2018 r. odbyły się coroczne warsztaty rozpatrywania spraw, w których uczestniczył przedstawiciel UODO.

6. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2018 r. GIODO/Prezes UODO i jego przedstawiciele uczestniczyli w konferencjach, seminariach i spotkania o charakterze międzynarodowym w kraju i za granicą.

Wykaz wydarzeń o charakterze międzynarodowym, które odbyły się w 2018 r. z udziałem GIODO/Prezesa UODO lub jego przedstawicieli znajduje się w załączniku nr 4., poniżej zaś przedstawione zostały wybrane przykłady najważniejszych wydarzeń.

1. Konferencja Miast Europejskich, Wiedeń (Austria), 6.03.2018 r.

W dniach 5–6 marca 2018 r. przedstawiciel GIODO/UODO uczestniczył w Konferencji Miast Europejskich poświęconej ochronie danych pt. „Data Protection 2018. Data & Democracy – Digital challenges for the cities", zorganizowanej w Wiedniu przez Biuro Miasta Wiednia.

2. Konferencja ERA dotycząca prawa ochrony danych UE, Bruksela (Belgia), 19–20.04.2018 r.

19–20 kwietnia 2018 r. odbyła się konferencja dotycząca prawa ochrony danych UE zorganizowana przez Akademię Prawa Europejskiego (ERA) w Brukseli, w której wziął udział przedstawiciel GIODO. Tematem przewodnim konferencji było RODO w kontekście komercyjnym. Podczas wydarzenia przedstawiciel GIODO wystąpił w charakterze mówcy podczas dyskusji przy okrągłym stole pt. „Internet Rzeczy, dane geolokalizacyjne i telekomunikacja – jak radzić sobie z zasadami RODO?".

3. Konferencja Privacy Laws & Business dotycząca krajowego wdrożenia RODO, Londyn (Wielka Brytania), 30.04.2018 r.

30 kwietnia 2018 r. przedstawiciel GIODO uczestniczył w Konferencji poświęconej krajowemu wdrożeniu RODO zorganizowanej przez Privacy Laws & Business w Brukseli. Celem Konferencji było dokonanie przeglądu krajowego wdrożenia RODO we Francji, Niemczech, Polsce oraz Hiszpanii. Podczas wydarzenia przedstawiciel GIODO wystąpił w panelu dotyczącym krajowego wdrożenia RODO.

4. Konferencja Europejskich Organów Ochrony Danych, Tirana (Albania), 2–4.05.2018 r.

W Tiranie 2–4 maja 2018 r. GIODO wraz ze swoim przedstawicielem wzięli udział w Wiosennej Konferencji Europejskich Organów Ochrony Danych zorganizowanej przez Rzecznika Informacji i Ochrony Danych Albanii.

Podczas wydarzenia omawiane były m.in. kwestie dotyczące kompetencji organów ochrony danych w zakresie nadzoru nad służbami wywiadowczymi, zakresu terytorialnego RODO, modernizacji Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (nr ETS 108, zwanej w skrócie „Konwencją 108") oraz ochrony danych osobowych w ramach współpracy policyjnej i sądowej.

Wśród innych zagadnień dyskutowanych podczas dorocznego spotkania europejskich organów ochrony danych znalazły się m.in. kwestie dotyczące wpływu europejskich standardów ochrony danych na standardy w tym zakresie w innych krajach, wyzwań w obszarze ochrony danych w związku z akcjami humanitarnymi oraz przyszłej struktury Konferencji Europejskich Organów Ochrony Danych. Podczas wydarzenia przedstawiciel GIODO przedstawił sprawozdanie z działań Grupy Państw Europy Środkowej i Wschodniej (CEEDPA).

5. Spotkanie z przedstawicielem Frontexu w siedzibie UODO, Warszawa, 7.06.2018 r.

7 czerwca 2018 r. w siedzibie UODO w Warszawie odbyło się spotkanie z przedstawicielem Frontexu, mającym pełnić rolę przyszłego inspektora ochrony danych w tej instytucji. Celem spotkania była dyskusja dotycząca bezpieczeństwa danych pracowników Frontexu w wypełnianych przez nich Ankietach Bezpieczeństwa Osobowego.

6. Spotkanie poświęcone praktycznym aspektom wdrażania RODO, Samorin (Słowacja), 12–13.06.2018 r.

Przedstawiciele UODO wzięli udział we wspólnym spotkaniu organów ochrony danych z Polski, Słowacji i Węgier, które odbyło się 12–13 czerwca 2018 r. Podczas spotkania zorganizowanego przez Urząd Ochrony Danych Osobowych Republiki Słowackiej, przedstawiciele organów ochrony danych dyskutowali na bieżące tematy związane z praktycznymi aspektami wdrażania przepisów ogólnego rozporządzenia o ochronie danych (RODO). Spotkanie było o tyle istotne, że biorący w nim udział przedstawiciele Grupy Wyszehradzkiej mieli na celu omówienie praktycznych problemów i pytań, które pojawiły się w ciągu pierwszych kilku tygodni stosowania RODO.

Przedmiotem dyskusji były m.in. następujące zagadnienia:

- praktyczne rozwiązanie problemu różnicy wieku w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku w różnych państwach członkowskich;
- kwestia, czy nakładanie administracyjnych kar pieniężnych jest obowiązkiem organów;
- test proporcjonalności w kontekście uzasadnionego interesu administratora a prawa i wolności osób, których dane dotyczą;
- rozumienie wyrażenia *wspólna certyfikacja*, o której mowa w art. 42 ust. 5 RODO;
- realny wymiar zwolnienia dla małych i średnich przedsiębiorców, o którym mowa w art. 30 ust. 5 w kontekście motywu 13 RODO i stanowiska Grupy Roboczej Art. 29.

Ponadto uczestnicy spotkania wymienili się pierwszymi doświadczeniami związanymi z funkcjonowaniem systemu IMI będącego platformą wymiany informacji pomiędzy organami państw członkowskich w związku z mechanizmem współpracy i spójności, o których mowa w Rozdziale VII RODO.

7. 36. posiedzenie plenarne Komitetu T-PD, Strasburg (Francja), 19–21.06.2018 r.

19–21 czerwca 2018 roku Strasburgu odbyło się 36. posiedzenie plenarne Komitetu Konsultacyjnego ds. Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitetu T-PD), udział wzięli Prezes UODO wraz z przedstawicielem UODO.

Członkiem Komitetu T-PD z ramienia Rzeczypospolitej Polskiej jest Prezes UODO. Uczestnicy posiedzenia zapoznali się z informacjami dotyczącymi modernizacji Konwencji 108 i potwierdzili chęć przyjęcia Protokołu zmieniającego Konwencję 108 z 18 maja 2018 r. Komitet przyjął również informację na temat odroczenia terminu otwarcia do podpisu Protokołu, wzywając do szybkiego ustalenia daty ceremonii otwarcia do podpisu tego dokumentu, i następnie pilnego podpisania go i ratyfikowania przez strony Konwencji.

Podczas obrad przeanalizowano szereg dokumentów, m.in. projekt zalecenia w sprawie ochrony danych związanych ze zdrowiem, wstępne sprawozdanie w sprawie sztucznej inteligencji oraz projekt opinii w sprawie zgodności Porozumienia ICDPPC (w tym jego harmonogramu) z Konwencją 108+. Jednym z punktów posiedzenia planarnego było wspólne posiedzenie z Komitetem Sterującym ds. Mediów i Społeczeństwa Informacyjnego, które wspólnie zatwierdziły „Wytyczne dotyczące ochrony prywatności w mediach".

Dodatkowo członkowie posiedzenia zapoznali się z informacjami przedstawionymi przez Sekretariat w sprawie wniosku o przystąpienie ze strony Republiki Kazachstanu, który podkreślił znaczenie szybkiego przygotowania opinii w tej sprawie.

Komitet Konsultacyjny przyjął nowe wydanie podręcznika dotyczącego europejskiej ochrony danych, przygotowanego wspólnie przez Radę Europy, Agencję Praw Podstawowych Unii Europejskiej, mającego na celu integrację ostatniej aktualizacji zarówno prawa UE, jak i Rady Europy z najnowszym orzecznictwem Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej. Ponadto podczas obrad delegacje zapoznały się z finalizacją ustanowienia nagrody im. Stefano Rodotà.

8. Warsztaty CIPL dotyczące rozliczalności zgodnie z RODO, Paryż (Francja), 5.10.2018 r.

5 października 2019 r. przedstawiciel Urzędu Ochrony Danych Osobowych uczestniczył w warsztatach pt. „Rozliczalność zgodnie z RODO – sposoby wdrażania, wykazywania i zachęcania do stosowania tej zasady" zorganizowanych przez Centre for Information Policy Leadership (CIPL) w Paryżu. Wystąpił on w charakterze mówcy w sesji poświęconej kwestii związanej z wykazywaniem przez organizacje rozliczalności, zarówno wobec organów ochrony danych, jak i wewnątrz organizacji.

9. Ceremonia otwarcia do podpisu Protokołu zmieniającego Konwencję 108, Strasburg (Francja), 10.10.2018 r.

10 października 2018 r. w Strasburgu odbyła się ceremonia otwarcia do podpisu Protokołu zmieniającego Konwencję 108, mającego na celu wzmocnienie zasad i reguł ochrony danych osobowych na szczeblu międzynarodowym. Protokół aktualizuje Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, zwaną również Konwencją 108, która jest jedynym istniejącym traktatem międzynarodowym, dotyczącym prawa jednostek do ochrony ich danych osobistych. Protokół ten wzmacnia zasady ochrony danych Konwencji 108 i obejmuje dodatkowe zabezpieczenia w celu sprostania wyzwaniom związanym z ochroną danych osobowych wynikającym z nowych technologii i praktyk. Rozszerza również rolę Komitetu Konwentu, który będzie monitorował, czy Strony skutecznie wdrażają postanowienia zaktualizowanego traktatu. Zmodernizowana konwencja, którą eksperci w dziedzinie ochrony danych nazywają Konwencją 108+, ma na celu zapewnienie, że przekazywanie danych osobowych przez granice odbywa się za pomocą odpowiednich zabezpieczeń oraz że jest ona zgodna z normatywnymi ramami na całym świecie, w tym z europejskim ustawodawstwem. Zmieniony traktat zapewnia również możliwość przystąpienia do niego Unii Europejskiej i organizacji międzynarodowych. Przykłady najważniejszych innowacji zawartych w Protokole:

- mocniejsze wymogi dotyczące zasad proporcjonalności i minimalizacji danych oraz zgodności z prawem przetwarzania;

- rozszerzenie rodzajów danych wrażliwych, które będą teraz obejmować dane genetyczne i biometryczne, przynależność do związków zawodowych i pochodzenie etniczne;
- obowiązek zgłaszania naruszeń danych;
- większa przejrzystość przetwarzania danych;
- nowe prawa dla osób w kontekście podejmowania decyzji algorytmicznych, które są szczególnie istotne w związku z rozwojem sztucznej inteligencji;
- większa odpowiedzialność administratorów;
- wymóg stosowania zasady „poszanowania prywatności od samego początku";
- stosowanie zasad ochrony danych do wszystkich działań związanych z przetwarzaniem, w tym ze względów bezpieczeństwa narodowego, z ewentualnymi wyjątkami i ograniczeniami, z zastrzeżeniem warunków określonych przez Konwencję, a w każdym razie z niezależną i skuteczną kontrolą i nadzorem;
- jasny reżim transgranicznych przepływów danych;
- wzmocnione uprawnienia i niezależność organów ochrony danych oraz poprawa podstaw prawnych dla współpracy międzynarodowej.

Prezes UODO z zadowoleniem przyjął informację, że na odbywającym się 16 maja 2019 r. w Helsinkach Szczycie, Minister Spraw Zagranicznych, prof. dr hab. Jacek Czaputowicz, podpisał Protokół zmieniający Konwencję o ochronie osób w związku z przetwarzaniem danych osobowych[215].

10. Konferencja dotycząca RODO, prawidłowych zasad ochrony danych i perspektyw na przyszłość, Szeged (Węgry), 18.10.2018 r.

18 października 2018 r. przedstawiciel UODO uczestniczył w Konferencji poświęconej RODO, prawidłowym zasadom ochrony danych i perspektywom na przyszłość, zorganizowanej przez Uniwersytet w Szeged, na Węgrzech. Podczas wydarzenia przedstawiciel UODO wygłosił wystąpienie pt. „Wyzwania związane z zapewnianiem zgodności z RODO w Polsce – punkt widzenia krajowego organu nadzorczego".

11. 40. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności, Bruksela (Belgia), 22–26.10.2018 r.

Przyjęciem pięciu rezolucji i deklaracji zakończyła się 40. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności obradująca od 22 do 26 października 2018 r. w Brukseli.

Gospodarzem 40. Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności był Europejski Inspektor Ochrony Danych, Giovanni Buttarelli, zaś jej współorganizatorem – Komisja Ochrony Danych Osobowych Republiki Bułgarii, która w Sofii zorganizowała wydarzenia towarzyszące. Urząd Ochrony Danych Osobowych reprezentowały Prezes UODO oraz przedstawiciel UODO.

Konferencja została podzielona na dwie sesje: zamkniętą oraz publiczną.

Sesja zamknięta odbyła się 22–23 października 2018 r. i uczestniczyli w niej akredytowani członkowie (m.in. przedstawiciele organów ochrony danych osobowych) oraz obserwatorzy Konferencji. Ta część wydarzenia rozpoczęła się od przyjęcia nowych członków – organów ochrony danych Dolnej Saksonii, Niemcy (Die Landesbeauftragte fuer den Datenschutz); Bawarii, Niemcy (Bayerisches Landesamt für Datenschutzaufsicht); Argentyny (Agencia de Acceso a la Información Pública) oraz Republiki Korei (Korea Communications Commission).

[215] Schemat podpisów i ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dostępny jest tutaj: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

Na sesji zamkniętej uchwalono następujące dokumenty:
Rezolucję w sprawie platform e-learningowych,
Deklarację w sprawie etyki i ochrony danych w zakresie sztucznej inteligencji,
Rezolucję w sprawie zmiany zasad i procedur obowiązujących w Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności,
Rezolucję w sprawie przyszłych działań dotyczących Międzynarodowej Konferencji Rzeczników Ochrony Danych Osobowych i Prywatności,
Rezolucję w sprawie współpracy między organami ochrony danych osobowych a organami ochrony konsumentów na rzecz lepszej ochrony obywateli i konsumentów w gospodarce cyfrowej,
Rezolucję w sprawie spisu powszechnego.

Sesja publiczna, w której mogli uczestniczyć zarówno członkowie sesji zamkniętych, jak i przedstawiciele sektora publicznego i prywatnego, odbyła się 24–26 października 2018 r.
Przedmiotem dyskusji podczas sesji była etyka cyfrowa, w tym kwestie takie jak godność i szacunek w życiu, w którym rządzą dane.
Tradycyjnie w tym samym czasie odbyły się również 44 wydarzenia towarzyszące Międzynarodowej Konferencji (tzw. *side events*).

12. Seminarium Naukowe poświęcone aktualnym problemom prawa pracy. Organizator: Uniwersytet w Oslo, Oslo (Norwegia), 13.11.2018 r.

W dniu 13 listopada 2018 r. odbyło się w Oslo seminarium norweskiego Forum Pracy poświęcone aktualnym problemom prawa pracy. Przedstawiciel UODO został zaproszony przez organizatorów do wygłoszenia referatu dotyczącego współczesnego paradygmatu prawa do prywatności pracowników w Europie i na świecie. Prezentacja ta miała miejsce w odrębnym panelu poświęconym prawu do prywatności w zatrudnieniu, w ramach którego przedstawione zostały również wybrane problemy dotyczące ochrony danych osobowych pracowników w Norwegii na gruncie RODO. Dyskusję zdominowała problematyka art. 88 RODO, tj. zasadności wprowadzenia przez państwa członkowskie do porządków krajowych, komplementarnych w stosunku do przepisów RODO przepisów prawnych dotyczących ochrony danych osobowych w zatrudnieniu (w tym w szczególności w odniesieniu do rekrutacji czy szeroko rozumianego monitorowania pracowników), a także kwestia interpretacji poszczególnych przepisów RODO w kontekście zatrudnienia (m.in. pojęcie danych osobowych, administratora, zasady przetwarzania danych, przesłanki legalności przetwarzania danych osobowych).

13. 37. posiedzenie plenarne Komitetu T-PD. Strasburg (Francja), 19–21.11.2018 r.

Uczestnicy posiedzenia zapoznali się z informacjami dotyczącymi ceremonii otwarcia do podpisu protokołu zmieniającego Konwencję 108, która odbyła się 10 października 2018 r. Delegacje zostały wezwane do działania na poziomie krajowym, aby doprowadzić do szybkiego wejścia w życie Konwencji 108+. Dodatkowo specjalny organ ONZ – sprawozdawca ds. prawa do prywatności zaapelował, aby państwa członkowskie ONZ przystąpiły do Konwencji 108+.

Omawiano również zagadnienia dotyczące m.in. prac podjętych przez Radę Europy w dziedzinie sztucznej inteligencji, znaczenia współpracy z firmami internetowymi i stowarzyszeniami, które podpisały list z Sekretarzem Generalnym Organizacji, możliwych ścieżek dla Komitetu Konwencji nr 108, bezpośredniej komunikacji i raportowania do Komitetu Ministrów lub jednej z grup sprawozdawców ds. Prac Komitetu. Delegacje zapoznały się także z informacjami przekazanymi przez Sekretariat w sprawie modernizacji Konwencji nr 108, w szczególności w odniesieniu do art. 37 protokołu zmieniającego CETS nr 223 w dniu wejścia w życie Konwencji 108+.

Komitet zapoznał się z prezentacją przedstawioną przez Christophera Dockseya, Honorowego Dyrektora Generalnego EIOD w sprawie najnowszego orzecznictwa Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej, jak również z informacjami dostarczonymi przez Eduardo Bertoniego, które dotyczyły międzyamerykańskiego systemu praw człowieka w dziedzinie ochrony prywatności i danych osobowych.

Delegacje posiedzenia planarnego odnotowały ustanowienie nagrody im. Stefano Rodotà z zamiarem przyznania jej po raz pierwszy z okazji Europejskiego Dnia Ochrony Danych w 2019 r. oraz zostały poproszone o dalsze przekazywanie informacji o możliwości składania wniosków przez kandydatów[216].

20. Spotkanie Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA). Kijów (Ukraina), 27–29.11.2018 r.

Gospodarzem wydarzenia był Sekretariat Komisarza ds. Praw Człowieka Ukraińskiego Parlamentu. Zgodnie z nowelizacją ukraińskiej ustawy o ochronie danych osobowych, wprowadzonej w 2014 r., sprawowanie kontroli nad przestrzeganiem przepisów o ochronie danych osobowych zostało powierzone ukraińskiemu Komisarzowi ds. Praw człowieka. Wśród uczestników spotkania znaleźli się przewodniczący i przedstawiciele organów ochrony danych z państw członkowskich CEEDPA. Uczestnicy mieli możliwość wymiany doświadczeń i najlepszych praktyk podczas dyskusji na temat kluczowych aspektów dotyczących ochrony danych osobowych, dotychczasowych osiągnięć i wyzwań.

Przedmiotem dyskusji panelowych były następujące kwestie: podsumowanie pierwszych sześciu miesięcy praktycznego stosowania rozporządzenia ogólnego o ochronie danych, zmodernizowana Konwencja w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych czy też wymiana praktycznych doświadczeń zdobytych dzięki stosowaniu przepisów w dziedzinie ochrony danych osobowych. Swoimi doświadczeniami szerzej w odrębnym panelu podzielili się gospodarze spotkania. Podczas spotkania debatowano także na temat wewnętrznych zasad CEEDPA i przyszłej współpracy. W związku z wprowadzeniem w przeddzień spotkania stanu wojennego na Ukrainie, zdecydowano o odwołaniu wyjazdu polskiej delegacji.

[216] Więcej informacji o 37. posiedzeniu plenarnym Komitetu T-PD dostępnych jest na stronie: https://rm.coe.int/37th-t-pd-plenary-meeting-abridged-report/16808fec2f .

ZAŁĄCZNIKI

Załącznik nr 1. Wykaz szkoleń przeprowadzonych przez UODO w 2018 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	11.01.2018	Warszawa	Szkolenie dla podmiotów zainteresowanych opracowaniem kodeksu postępowania w świetle RODO
2.	22.01.2018	Kielce	Wojewódzki Urząd Pracy w Kielcach
3.	16.02.2018	Białystok	Podlaski Urząd Wojewódzki
4.	27.02.2018	Warszawa	ABI sektora szkolnictwa i oświaty
5.	16.03.2018	Kraków	Urząd Marszałkowski Województwa Małopolskiego
6.	22.03.2018	Warszawa	Ministerstwo Finansów
7.	5.04.2018	Warszawa	Forum Zarządzania Publicznego, KSAP
8.	6.04.2018	Warszawa	Wykład online TDTS
9.	9.04.2018	Warszawa	Wykład online pt. „Inspektor ochrony danych – fachowy doradca i audytor obowiązkowy w każdej szkole”
10.	24.04.2018	Warszawa	ABI sektora przedszkoli
11.	26.04.2018	Rzeszów	Organizacje pozarządowe województwa podkarpackiego
12.	9.05.2018	Piła	Administracja publiczna regionu Północnej Wielkopolski
13.	10.05.2018	Gorzów Wielkopolski	Organizacje pozarządowe województwa lubuskiego
14.	11.05.2018	Poznań	Organizacje pozarządowe województwa wielkopolskiego
15.	17.05.2018	Warszawa	NSZZ „Solidarność”
16.	18.05.2018	Wrocław	Dolnośląski Urząd Wojewódzki
17.	21.05.2018	Kielce	Organizacje pozarządowe województwa świętokrzyskiego
18.	21.05.2018	Kielce	Świętokrzyski Urząd Wojewódzki
19.	4.06.2018	Warszawa	Kancelaria Sejmu RP
20.	12.06.2018	Kielce	Ekonomowie i Sekretarze Prowincjonalnych Zakonów w Polsce
21.	14.06.2018	Warszawa	Przedstawiciele mniejszości narodowych i etnicznych (MSWiA)
22.	18.06.2018	Warszawa	Kancelaria Premiera Rady Ministrów – konsultacje
23.	21.06.2018	Bydgoszcz	Organizacje pozarządowe województwa kujawsko-pomorskiego
24.	22.06.2018	Toruń	Organizacje pozarządowe województwa kujawsko-pomorskiego
25.	26.06.2018	Warszawa	IOD sektora mieszkalnictwa
26.	27.06.2018	Wrocław	Jednostki samorządu terytorialnego województwa dolnośląskiego
27.	28.06.2018	Gdańsk	Organizacje pozarządowe województwa pomorskiego
28.	28.06.2018	Opole	Jednostki samorządu terytorialnego województwa opolskiego

29.	29.06.2018	Katowice	Jednostki samorządu terytorialnego województwa śląskiego
30.	05.09.2018	Legnica	Przedstawiciele MŚP regionu Dolnego Śląska
31.	05.09.2019	Legnica	Organizacje pozarządowe województwa dolnośląskiego
32.	06.09.2018	Opole	Organizacje pozarządowe województwa opolskiego
33.	06.09.2018	Katowice	Organizacje pozarządowe województwa śląskiego
34.	07.09.2018	Kraków	Organizacje pozarządowe województwa małopolskiego
35.	07.09.2018	Kraków	Jednostki samorządu terytorialnego województwa małopolskiego
36.	20.09.2018	Warszawa	Ministerstwo Rodziny, Pracy i Polityki Społecznej
37.	01.10.2018	Lublin	Organizacje pozarządowe województwa lubelskiego
38.	02.10.2018	Jachranka	Sędziowie WSA w Warszawie
39.	02.10.2018	Warszawa	IOD placówek oświatowych trzech dzielnic Warszawy
40.	4.10.2018	Gdańsk	Dyrektorzy WUP i agencji zatrudnienia
41.	04.10.2018	Warszawa	IOD sektora zatrudnienia
42.	11.10.2018	Łódź	Organizacje pozarządowe województwa łódzkiego
43.	15.10.2018	Warszawa	Szkolenie uczestników programu TDTS
44.	23.10.2018	Białystok	Organizacje pozarządowe województwa podlaskiego
45.	25.10.2018	Szczecin	Organizacje pozarządowe województwa zachodnio-pomorskiego
46.	15.11.2018	Szczecin	Jednostki samorządu terytorialnego województwa zachodnio-pomorskiego
47.	16.11.2018	Zielona Góra	Jednostki samorządu terytorialnego województwa lubuskiego
48.	22.11.2018	Kielce	Jednostki samorządu terytorialnego województwa świętokrzyskiego
49.	07.12.2018	Białystok	Jednostki samorządu terytorialnego województwa podlaskiego
50.	19.12.2018	Warszawa	IOD – ocena skutków dla ochrony danych
51.	20.12.2018	Warszawa	Studenci Wydziału Farmacji Warszawskiego Uniwersytetu Medycznego

Załącznik nr 2. Wykaz wydarzeń objętych patronatem Prezesa UODO w 2018 r.

1. Konferencja z okazji obchodów XII Dnia Ochrony Danych Osobowych, pt. „Administrator danych osobowych w perspektywie RODO". Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 30.01.2018 r.
2. Konferencja pt. „ABI w nowej roli – inspektor ochrony danych", zorganizowana w ramach obchodów XII Dnia Ochrony Danych Osobowych przez Stowarzyszenie Administratorów Bezpieczeństwa Informacji (SABI) oraz Wydział Zarządzania Politechniki Warszawskiej. Warszawa, 30.01.2018 r.
3. Konferencja Naukowa pt. „Od ustawy ODO do RODO" zorganizowana z okazji XII Dnia Ochrony Danych Osobowych przez Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi Collegium Civitas. Zamek Królewski w Warszawie, 15.02.2018 r.
4. Konferencja Naukowa pt. „Bezpieczeństwo danych osobowych w cyberprzestrzeni: szanse, wyzwania, zagrożenia", organizowana w ramach obchodów XII Dnia Ochrony Danych Osobowych przez Akademię Marynarki Wojennej im. Obrońców Westerplatte w Gdyni. Gdynia, 28.02.2018 r.
5. Konferencja pt. "Tajemnica medyczna. Praktyczne dylematy ochrony danych pacjentów". Organizatorzy: Okręgowa Izba Lekarska w Warszawie, Naczelna Izba Lekarska w Warszawie, Naczelna Izba Położnych i Pielęgniarek w Warszawie, Okręgowa Izba Pielęgniarek i Położnych w Warszawie oraz Okręgowa Izba Pielęgniarek i Położnych w Radomiu. Warszawa, 5.03.2018 r.
6. Konferencja Naukowa pt. "Bezpieczeństwo informacji w sektorze ochrony zdrowia. Wdrożenie RODO w sektorze ochrony zdrowia". Organizator: Śląski Uniwersytet Medyczny w Katowicach. Katowice, 6.03.2018 r.
7. III edycja Economic Security Forum ECONSEC 2018 „Bezpieczeństwo narodowe i gospodarcze wobec cyberzagrożeń". Organizator: Europejskie Centrum Biznesu, Warszawa, 15.032018 r.
8. Ogólnopolska Konferencja Naukowa – IV Forum Prawa Mediów Elektronicznych. Organizator: Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Wrocław, 10–11.04.2018 r.
9. GIODO członkiem Komitetu Honorowego obchodów 70-lecia informatyki w Polsce oraz Światowego Dnia Społeczeństwa Informacyjnego w Polsce (ŚDSI) w 2018 r.
10. XIII Ogólnopolski Zjazd Kół Naukowych przy Wydziałach Prawa i Administracji pt. „Prawo do prywatności w obliczu wyzwań współczesnego świata". Organizator: Koło Naukowe Prawa Pracy przy Katedrze Prawa Pracy Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 24–25.04.2018 r.
11. Kampania informacyjna „Gotowi na RODO". Organizator: Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Informacyjnego we współpracy z UODO. Termin realizacji: 26.04.–30.11.2018 r.
12. Konferencja szkoleniowa dla przedstawicieli administracji publicznej z regionu Północnej Wielkopolski. Organizator: Prezydent Miasta Piły. Piła, 9.05.2018 r.
13. Konferencja „Ochrona Danych Osobowych w świetle rozporządzenia o ochronie danych RODO" w ramach cyklu konferencji „Cywilizacyjne wyzwania Informatyki". Organizator: Akademia im. Jakuba z Paradyża, Gorzów Wielkopolski, 10.05.2018 r.
14. Konferencja Naukowa „Ogólne rozporządzenie o ochronie danych (RODO). Nowe wyzwania dla radcy prawnego w zakresie ochrony danych osobowych". Organizator: Okręgowa Izba Radców Prawnych w Krakowie oraz Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego, Kraków, 10–11.05.2018 r.

15. V edycja konferencji „Security Case Study – SCS 2018”. Organizator: Fundacja Bezpieczna Cyberprzestrzeń, Warszawa, 13–14.09.2018 r.
16. Konferencja Naukowa „Pozycja prawna inspektora ochrony danych osobowych (IODO)”. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego. Łódź, 28.09.2018 r.
17. III Forum Bezpieczeństwa IT w Administracji. Organizator: Redakcja miesięcznika „IT w Administracji”. Jastrzębia Góra, 10–12.10.2018 r.
18. IV edycja Ogólnopolskiego Szczytu Gospodarczego OSG 2018 „Państwo – Gospodarka – Bezpieczeństwo: Filary polskiej gospodarki przyszłości”. Organizator: Europejskie Centrum Biznesu. Siedlce, 18–19.10.2018 r.
19. XXII Kongres Polskiej Federacji Rynku Nieruchomości. Organizator: Warszawskie Stowarzyszenie Pośredników w Obrocie Nieruchomościami. Warszawa, 26.10.2018 r.
20. Cyfrowa Wyprawka Fundacji Panoptykon, 2018.
21. VII edycja Konwentu Ochrony Danych Osobowych i Informacji. Organizator: Lubasz i Wspólnicy Kancelaria Radców Prawnych, Forsafe Sp.z o .o. Łódź, 23.11.2018 r.
22. Kongres Impact fintech’18. Organizator: Fundacja Impact. Łódź, 28–29.11.2018 r.
23. Konferencja Naukowa pt. „Zasady przetwarzania danych osobowych w sferze zatrudnienia”. Organizator: Zakład Prawa Pracy Akademii Leona Koźmińskiego w Warszawie. Warszawa, 4.12.2018
24. Ogólnopolska Konferencja Naukowa pt. „Dane biometryczne a prawo do prywatności informacyjnej pracowników”. Organizatorzy: Zakład Prawa Pracy i Zabezpieczenia Społecznego Uniwersytetu Opolskiego, Okręgowa Izba Radców Prawnych w Opolu oraz Fundacja Radców Prawnych B2B w Opolu. Opole, 13 grudnia 2018 r.

Załącznik nr 3. Wykaz konferencji, seminariów i spotkań krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2018 r. w Polsce przez UODO lub inne podmioty

L.p.	Data	Konferencja/Seminarium	Miejsce
1.	04.01.2018	IV Ogólnopolska Konferencja „Podkarpacie dla biznesu" , Organizator: Oddział ZUS w Rzeszowie i Izba Administracji Skarbowej w Rzeszowie.	Rzeszów
2.	18.01.2018	Spotkanie ekspertów organu ochrony danych z przedstawicielami firmy Billon, która opracowała unikalne na świecie rozwiązania opierające się na technologii blockchain.	Warszawa
3.	29.01.2018	XII Dzień Ochrony Danych Osobowych. Konferencja „Zainwestuj w prywatność. Przygotowujemy się do #RODO". Organizator: GIODO	Warszawa
4.	30.01.2018	Konferencja Naukowa pt. „Administrator danych osobowych w perspektywie RODO". Organizator: Centrum Ochrony Danych i Zarządzania Informacja na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
5.	15.02.2018	Konferencja pt. „Od ustawy ODO do RODO". Organizator: Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi Collegium Civitas.	Warszawa
6.	26.02.2018	Posiedzenie Senatu Warszawskiego Uniwersytetu Medycznego z okazji XII Dnia ochrony Danych Osobowych 2018	Warszawa
7.	5.03.2018	Konferencja Rektorów Polskich Uczelni Technicznych. Organizator: Politechnika Śląska	Warszawa
8.	6.03.2018	Konferencja „Bezpieczeństwo informacji w sektorze ochrony zdrowia w świetle RODO". Organizator: Śląski Uniwersytet Medyczny w Katowicach	Katowice
9.	14.03.2018	XIII Ogólnopolski Kongres PERTOBIZNES Paliwa, Chemia, Gaz. Organizator: Europejskie Centrum Biznesu.	Warszawa
10.	15.03.2018	3. edycja Economic Security Forum ECONOSEC 2018 pt. „Bezpieczeństwo narodowe i gospodarcze wobec cyberzagrożeń". Organizator: Europejskie Centrum Biznesu	Lublin
11.	15.03.2018	Sympozjum Naukowe pt. „Prawo do prywatności w Kościołach i innych związkach wyznaniowych: od tajemnicy duszpasterskiej do ochrony danych osobowych". Organizator: CHAT – Chrześcijańska Akademia Teologiczna w Warszawie.	Warszawa
12.	16.03.2018	XX posiedzenie Rady Konsultacyjnej ds. Ochrony Konsumentów. Organizator: Urząd Marszałkowski Województwa Małopolskiego	Kraków
13.	19.03.2018	Konferencja Rektorów Uczelni Pedagogicznych. Organizator: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach	Siedlce
14.	22.03.2018	Spotkanie z audytorami wewnętrznymi jednostek administracji rządowej i samorządowej. Organizator: Ministerstwo Finansów.	Warszawa
15.	27.03.2018	Szkolenie z tematyki RODO dla kierowników wojewódzkich samorządowych jednostek organizacyjnych. Organizator: Urząd Marszałkowski Województwa. Mazowieckiego.	Warszawa
16.	09.04.2018	Konferencja „Bezpieczeństwo danych – problemy prawne i techniczne". Organizator: GUS, ZUS oraz Wojskowa Akademia Techniczna	Warszawa
17.	10–11.04.2018	IV Forum Prawa Mediów Elektronicznych. Organizator: Centrum Badań Problemów Prawnych i Ekonomicznych	Wrocław

		Komunikacji Elektronicznej Wydziału Prawa Administracji i Ekonomii Uniwersytetu Wrocławskiego	
18.	12.04.2018	Warsztaty dla nauczycieli w ramach konkursu „Mój pierwszy telefon – ochrona prywatności w sieci". Organizator: UODO, Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie	Warszawa
19.	14.04.2018	Konferencja Uniwersyteckich Poradni Prawnych w Słubicach. Organizator: Koło Naukowe Studenckiej Poradni Prawa Collegium Polonicum w Słubicach	Słubice
20.	18–19.04.2018	X Ogólnopolski Kongres Prawa Bankowego. Organizator: Koło Naukowe Prawa Bankowego przy Uniwersytecie Warszawskim.	Warszawa
21.	23.04.2018	X Międzynarodowa Konferencja Naukowa „Powszechne i regionalne systemy praw człowieka 70 lat po proklamowaniu Powszechnej Deklaracji Praw Człowieka". Organizator: Uniwersytet Jana Kochanowskiego w Kielcach oraz Zarząd Główny Stowarzyszenia Parlamentarzystów Polskich	Warszawa
22.	24.04.2018	Konferencja „Świat po RODO – rozważania, rozwiązania". Organizator: Fundacja Bezpieczna Cyberprzestrzeń	Warszawa
23.	25–27.04.2018	Seminarium szkoleniowe pn. „Problematyka stosowania przepisów prawa w dziedzinie geodezji i kartografii". Organizator: Stowarzyszenie Geodetów Polskich.	Falenty
24.	27.04.2018	XII Ogólnopolska Konferencja Społeczności Centrum Europejskiego Uniwersytetu Warszawskiego pt. „Wojny w czasach cyfrowej rewolucji"	Warszawa
25.	09.05.2018	Konferencja dla przedstawicieli administracji publicznej z regionu Północnej Wielkopolski. Organizatorzy: Prezydent Miasta Piła.	Piła
26.	10.05.2018	Konferencja Ochrona Danych Osobowych w świetle rozporządzenia o ochronie danych (RODO) w ramach cyklu konferencji „Cywilizacyjne wyzwania Informatyki". Organizator: Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim i Lubuski Urząd Wojewódzki	Gorzów Wlk.
27.	21.05.2018	Szkolenie z zakresu zagadnień RODO dla kadry zarządzającej Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach	Kielce
28.	25.05.2018	X Konferencja z cyklu „Bezpieczeństwo w Internecie", pt. „Przetwarzanie danych osobowych". Organizatorzy: UKSW, UODO, Naukowe Centrum Prawno-Informatyczne.	Warszawa
29.	04.06.2018	XX Szkoła Zarządzania Strategicznego w szkolnictwie wyższym dla Kanclerzy i Kwestorów/Dyrektorów Finansowych. Organizator: Fundacja rektorów Polskich i Konferencja Rektorów Akademickich Szkół Polskich (KRASP)	Janów Podlaski
30.	8.06.2018	Konferencja podsumowująca 8. edycję programu „Twoje dane – Twoja sprawa". Organizator: UODO	Warszawa
31.	11–13.06.2018	Konferencja Wyższych Przełożonych Zakonów Męskich w Polsce, spotkanie sekretarzy i ekonomów, SACROEXPO	Kielce
32.	20–21.06.2018	Konferencja „Technology Risk Management Forum". Organizator: Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych ISSA Polska	Wrocław
33.	22.06.2018	Konferencja „Nowe regulacje w zakresie ochrony danych osobowych". Organizator: Wydział Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu	Toruń
34.	26.06.2018	Konferencja „Bezpieczeństwo danych firmowych w rzeczywistości RODO. Organizator: Wydział Nauk prawnych Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach.	Siedlce

35.	27.06.2018	V Ogólnopolskie Seminarium Sekretarzy. Organizatorzy: Redaktor Naczelny Pisma Samorządu Terytorialnego „WSPÓLNOTA” oraz Municipium S.A.	Warszawa
36.	27–29.06.2018	XXII Konferencja Miasta w Internecie pod hasłem: ROK 2018: PUZZLE CYFROWEJ POLSKI – Miasta przyszłości – Technologie transformacji – Cyfrowa szkoła. Organizator: Stowarzyszenie Miasta w Internecie	Gdańsk
37.	28.06.2018	Konferencja eMEDit 2018. Technologie IT w medycynie. Organizator: Health Project Management	Warszawa
38.	3–4.07.2018	Międzynarodowa Konferencja „Prawa człowieka: ewaluacja i kierunki rozwoju”. Organizator: UKSW w Warszawie	Warszawa
39.	4–6.09.2018	XXVIII Forum Ekonomiczne w Krynicy – Zdrój pt. „Europa wspólnych wartości czy Europa wspólnych interesów?”. Organizator: Fundacja Instytut Studiów Wschodnich	Krynica Zdrój
40.	13–14.09.2018	V edycja konferencji „SECURITY CASE STUDY”. Organizator: Fundacja Bezpieczna Cyberprzestrzeń	Warszawa
41.	20.09.2018	Seminarium „Ochrona danych osobowych w świetle RODO dla sektora szkolnictwa wyższego – 2”. Organizator: Fundacja na Rzecz Jakości Kształcenia	Warszawa
42.	21.09.2018	Seminarium Naukowe „Ochrona danych osobowych w fazie projektowania. Wymogi RODO w tworzeniu oprogramowania”. Organizator: UODO	Warszawa
43.	27.09.2018	24. Forum Teleinformatyki. Organizator: BizTech.	Miedzeszyn k/Warszawy
44.	28.09.2018	Ogólnopolska Konferencja Naukowa pt. „Pozycja prawna inspektora ochrony danych osobowych”. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego.	Łódź
45.	28.09.2018	III Ogólnopolska Konferencja Naukowa z zakresu rejestracji stanu cywilnego w Polsce. Organizatorzy: UODO, KUL, NIST, PWPW.	Lublin
46.	02.10.2018	Konferencja Szkoleniowa Sędziów WSA w Warszawie. Organizator: Prezes Wojewódzkiego Sądu Administracyjnego w Warszawie.	Jachranka
47.	02.10.2018	Szkolenie dla IOD w placówkach oświatowych z terenu dzielnicy Praga Południe, Białołęka i Ursynów. Organizator: Dzielnicowe Biuro Finansów Oświaty Praga Południe oraz JAMANO sp. z o.o.	Warszawa
48.	03.10.2018	Konferencja „Seminarium sekretarzy” odbywająca się w ramach XVI Samorządowego Forum Kapitału i Finansów.	Katowice
49.	4.10.2018	Konferencja Szkoleniowa nt. wymiany danych osobowych pomiędzy instytucjami rynku pracy. Organizator: Wojewódzki Urząd Pracy w Gdańsku.	Gdańsk
50.	05.10.2018	Konferencja „Blockchain – bariery i transformacje”. Organizator: Towarzystwo Ekonomistów Polskich, Szkoła Główna Handlowa i Wydział Prawa Uniwersytet Jagielloński.	Warszawa
51.	10–12.10.2018	III Forum Bezpieczeństwa IT w Administracji. Organizator: Redakcja miesięcznika „IT w Administracji”.	Jastrzębia Góra
52.	18–19.10.2018	IV edycja Ogólnopolskiego Szczytu Gospodarczego OSG 2018 pt. „Państwo – Gospodarka –Bezpieczeństwo: Filary polskiej gospodarki przyszłości”. Organizator: Europejskie Centrum Biznesu	Siedlce
53.	19.10.2018	II Konferencja Naukowa „Bezpieczeństwo dokumentów publicznych”. Organizatorzy: WSP w Szczytnie oraz MSWiA	Szczytno

54.	22.10.2018	II Forum Informacji i Ochrony Danych Osobowych. Organizator: Redakcja kwartalnika „ABI Expert”.	Toruń
55.	23.10.2018	II Kongres RODO. Reforma ochrony danych osobowych – pierwsze doświadczenia”. Organizator: Wolters Kluwer	Warszawa
56.	26.10.2018	XXII Kongres Polskiej Federacji Rynku Nieruchomości, Warszawa. Organizator: Warszawskie Stowarzyszenie Pośredników w Obrocie Nieruchomościami.	Warszawa
57.	25–27.10.2018	Spotkanie szkoleniowo – warsztatowe dla Inspektorów Ochrony Danych. Organizator: Kościelny Inspektor Ochrony Danych i Konferencja Episkopatu Polski	Księżówka k/Zakopanego
58.	13–14.11.2018	Konferencja Advanced Threat Summit 2018. Organizatorzy: Evention i ISSA	Warszawa
59.	15.11.2018	3. ed. Kongresu 590 pt. „Nie takie RODO straszne? Bilans półrocza”. Organizator: Kongres 590 Sp. z o.o.	Jasionka k/Rzeszowa
60.	23.11.2018	VII Konwent Ochrony Danych i Informacji. Organizatorzy: Lubasz i Wspólnicy Kancelaria Radców Prawnych oraz Forsafe Sp. z o. o.	Łódź
61.	4.12.2018	I Kongres IOD pt. „Weryfikacja wdrożenia RODO”. Organizator: ENSI	Warka nad Pilicą
62.	4–5.12.2018	7 Kongres Prawa Medycznego. Organizator: Polskie Towarzystwo Prawa Medycznego	Kraków
63.	5.12.2018	Konferencja „Blockchain – bariery i transformacje”. Organizator: Towarzystwo Ekonomistów Polskich, Szkoła Główna Handlowa, Wydział Prawa Uniwersytetu Jagiellońskiego	Warszawa
64.	10.12.2018	„#RODO w edukacji. Mazowieckie spotkanie z ochroną danych osobowych w szkole”. Organizator: UODO	Przysucha
65.	13.12.2018	Ogólnopolska Konferencja Naukowa pt. „Dane biometryczne a prawo do prywatności informacyjnej pracowników”. Organizator: Zakład Prawa Pracy i Zabezpieczenia Społecznego Wydziału Prawa i Administracji Uniwersytetu Opolskiego.	Opole
66.	14.12.2018	VI Krajowe Forum Ochrony Infrastruktury Krytycznej. Organizator: Rządowe Centrum Bezpieczeństwa.	Warszawa
67.	20.12.2018	Wykład dla studentów Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego, w ramach przedmiotu: „Opieka farmaceutyczna”	Warszawa

Załącznik nr 4. Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, które odbyły się w 2018 r. za granicą

L.p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	10.01.2018	Posiedzenie Podgrupy ds. Współpracy (Cooperation) Grupy Roboczej Art. 29	Bruksela
2.	19.01.2018	Posiedzenie Podgrupy ds. eAdministracji (eGovernment) Grupy Roboczej Art. 29	Bruksela
3.	06–07.02.2018	114. posiedzenie Grupy Roboczej Art. 29 (Article 29 Working Party)	Bruksela
4.	08–09.02.2018	Spotkanie przyszłych użytkowników Systemu wymiany informacji na rynku wewnętrznym (Internal Market Information, IMI)	Bruksela
5.	05–06.03.2018	Konferencja Miast Europejskich	Wiedeń
6.	06–08.03.2018	Posiedzenie Podgrupy ds. Współpracy (Cooperation) Grupy Roboczej Art. 29	Bruksela
7.	12–14.03.2018	Pierwsze spotkanie partnerów projektu T4DATA (Training Data Protection Authorities and Data Protection Officers, Szkolenia dla Urzędów Ochrony Danych Osobowych i Inspektorów Ochrony Danych)	Zagrzeb
8.	14–15.03.2018	Spotkanie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
9.	14–15.03.2018	Posiedzenie Podgrupy ds. Kluczowych przepisów (Key Provisions) Grupy Roboczej Art. 29	Bruksela
10.	19–20.03.2018	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Grupy Roboczej Art. 29	Bruksela
11.	20–21.03.2018	Posiedzenie Podgrupy ds. Technologii (Technology) Grupy Roboczej Art. 29	Bruksela
12.	22–23.03.2018	Warsztaty Systemu wymiany informacji na rynku wewnętrznym (Internal Market Information, IMI)	Bruksela
13.	22.03.2018	Posiedzenie Podgrupy ds. eAdministracji (eGovernment) Grupy Roboczej Art. 29	Bruksela
14.	08–10.04.2018	Spotkanie Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (Grupa Berlińska)	Budapeszt
15.	09–11.04.2018	115. posiedzenie Grupy Roboczej Art. 29 (Article 29 Working Party)	Bruksela
16.	15–20.04.2018	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Bruksela
17.	15–20.04.2018	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Lizbona
18.	18–19.04.2018	Posiedzenie Podgrupy ds. Kluczowych przepisów (Key Provisions) Grupy Roboczej Art. 29	Bruksela
19.	19–20.04.2018	Konferencja Akademii Prawa Europejskiego (Academy of European Law, ERA) dot. prawa ochrony danych Unii Europejskiej	Bruksela
20.	24.04.2018	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers) Grupy Roboczej Art. 29	Bruksela
21.	25–26.04.2018	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Grupy Roboczej Art. 29	Bruksela
22.	25–27.04.2018	Szkolenie Systemu wymiany informacji na rynku wewnętrznym (Internal Market Information, IMI)	Bruksela
23.	29.04–01.05.2018	Konferencja Privacy Laws & Business dot. RODO	Londyn

24.	02.05.2018	Posiedzenie Podgrupy ds. eAdministracji (eGovernment) Grupy Roboczej Art. 29	Bruksela
25.	02–04.05.2018	Konferencja Europejskich Organów Ochrony Danych	Tirana
26.	03–04.05.2018	Warsztaty Systemu wymiany informacji na rynku wewnętrznym (Internal Market Information, IMI)	Bruksela
27.	06–11.05.2018	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Haga
28.	13–18.05.2018	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Paryż
29.	14–15.05.2018	Posiedzenie Podgrup Przyszłości Prywatności (Future of Privacy) oraz ds. Współpracy (Cooperation) Grupy Roboczej Art. 29	Bruksela
30.	23–25.05.2018	Posiedzenie Grupy Roboczej Art. 29 / Europejskiej Rady Ochrony Danych	Bruksela
31.	28–30.05.2018	IV Spotkanie partnerów projektu Erasmus	Skopje
32.	29.05.2018	Posiedzenie Systemów Informacji Celnej (Customs Information Systems, CIS)	Bruksela
33.	04–05.06.2018	Konferencja nt. ochrony prawa do prywatności w sieci	Bruksela
34.	07.06.2018	Posiedzenie Podgrupy ds. Kluczowych przepisów (Key Provisions) Europejskiej Rady Ochrony Danych	Bruksela
35.	10–14.06.2018	I międzynarodowy trening dla trenerów w ramach unijnego projektu T4DATA (Training Data Protection Authorities and Data Protection Officers, Szkolenia dla Urzędów Ochrony Danych Osobowych i Inspektorów Ochrony Danych)	Rzym
36.	11–13.06.2018	Spotkanie ws. Mechanizmu kompleksowej współpracy (One-stop-shop)	Šamorin
37.	18–21.06.2018	36. Posiedzenie plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD)	Strasburg
38.	04–05.07.2018	2. Posiedzenie plenarne Europejskiej Rady Ochrony Danych	Bruksela
39.	08–13.07.2018	Spotkanie w ramach projektu Erasmus	Ochryda
40.	10.07.2018	Posiedzenie Podgrupy ds. ds. Międzynarodowego Przekazywania Danych (International Transfers) Europejskiej Rady Ochrony Danych	Bruksela
41.	03–05.09.2018	Posiedzenie Podgrupy ds. Technologii (Technology) Europejskiej Rady Ochrony Danych	Bruksela
42.	05.09.2018	Posiedzenie Podgrupy ds. Współpracy (Cooperation) Europejskiej Rady Ochrony Danych	Bruksela
43.	05–06.09.2018	Spotkanie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Europejskiej Rady Ochrony Danych	Bruksela
44.	06–07.09.2018	Posiedzenie Podgrupy ds. Kluczowych przepisów (Key Provisions) Europejskiej Rady Ochrony Danych	Bruksela
45.	11.09.2018	Posiedzenie Podgrupy ds. Przyszłości Prywatności (Future of Privacy) Europejskiej Rady Ochrony Danych	Bruksela
46.	12–13.09.2018	Posiedzenie Podgrupy ds. eAdministracji (eGovernment) Europejskiej Rady Ochrony Danych	Bruksela
47.	13–14.09.2018	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media) Europejskiej Rady Ochrony Danych	Bruksela
48.	16–21.09.2018	Czynności kontrolne Systemu Informacyjnego Schengen	Tallin
49.	23–24.09.2018	Posiedzenie programowe Europejskiej Rady Ochrony Danych	Bruksela
50.	24–26.09.2018	3. Posiedzenie plenarne Europejskiej Rady Ochrony Danych	Bruksela
51.	02–03.10.2018	Posiedzenie dot. dozoru celnego oraz Europolu	Bruksela

52.	05.10.2018	Warsztaty Centre for Information Policy Leadership (CIPL) dot. zasady rozliczalności w RODO	Paryż
53.	10–11.10.2018	Posiedzenie Podgrupy ds. Użytkowników IT (IT Users) Europejskiej Rady Ochrony Danych	Bruksela
54.	16–17.10.2018	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers) Europejskiej Rady Ochrony Danych	Bruksela
55.	17–19.10.2018	Konferencja „Life after the GDPR: Good Data Protection Rules and Prospects for the Future"	Szeged
56.	18.10.2018	Posiedzenie Podgrupy ds. eAdministracji (eGovernment) Europejskiej Rady Ochrony Danych	Bruksela
57.	21–25.10.2018	Międzynarodowa Konferencja Komisarzy Ochrony Danych i Prywatności (International Conference of Data Protection & Privacy Commissioners, ICDPPC)	Bruksela
58.	06–07.11.2018	Posiedzenie Podgrupy ds. Technologii (Technology) Europejskiej Rady Ochrony Danych	Bruksela
59.	07–08.10.2018	Posiedzenie Podgrupy ds. Kluczowych przepisów (Key Provisions) Europejskiej Rady Ochrony Danych	Bruksela
60.	08–09.11.2018	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media) Europejskiej Rady Ochrony Danych	Bruksela
61.	12–14.11.2018	Posiedzenie Podgrupy ds. Współpracy (Cooperation) Europejskiej Rady Ochrony Danych	Bruksela
62.	12–17.11.2018	Wizyta w gruzińskim organie ochrony danych: Biurze Inspektora Ochrony Danych Osobowych (Office of the Personal Data Protection Inspector)	Tbilisi
63.	13.11.2018	Seminarium Naukowe nt. aktualnych problemów prawa pracy. Organizator: Uniwersytet w Oslo.	Oslo
64.	13–15.11.2018	Czynności kontrolne Wizowego Systemu Informacyjnego (VIS) oraz Systemu Informacyjnego Schengen (SIS II)	Bruksela
65.	14–15.11.2018	Posiedzenie Podgrupy ds. Nakładania Kar (Fining) Europejskiej Rady Ochrony Danych	Bruksela
66.	19–20.11.2018	Posiedzenie Podgrupy ds. eAdministracji (eGovernment) Europejskiej Rady Ochrony Danych	Bruksela
67.	19–22.11.2018	37. Posiedzenie plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD)	Strasburg
68.	27–29.11.2018	Complaints Handling Workshop – Warsztaty Skargowe (doroczne spotkanie organów ochrony danych z Europy, również spoza UE); gospodarz: NAIH (węgierski organ nadzorczy)	Budapeszt
69.	04–05.12.2018	5. Posiedzenie plenarne Europejskiej Rady Ochrony Danych	Bruksela
70.	09–11.12.2018	Spotkanie sprawozdawców Podgrupy ds. Technologii (Technology) Europejskiej Rady Ochrony Danych dot. wytycznych monitoringu wizyjnego	Berlin
71.	18–19.12.2018	Posiedzenie Podgrupy ds. Technologii (Technology) Europejskiej Rady Ochrony Danych	Bruksela