SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Prezes Urzędu Ochrony
Danych Osobowych
PU.060.1.2020

Druk nr 583

Warszawa, 20 sierpnia 2020 r.

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek

zgodnie z art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych przekazuję

- **Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019.**

Z wyrazami szacunku

(-) Jan Nowak

SPRAWOZDANIE Z DZIAŁALNOŚCI PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH W ROKU 2019

SPRAWOZDANIE Z DZIAŁALNOŚCI
PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
w ROKU 2019

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 oraz art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[1].

[1] Sprawozdanie obejmuje okres działalności Prezesa Urzędu Ochrony Danych Osobowych od 1 stycznia 2019 r. do 31 grudnia 2019 r.

Zgodnie z 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)[2], każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje środków podjętych 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[3], w myśl którego Prezes Urzędu Ochrony Danych Osobowych[4] 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 Urzędu 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).

[2] Dz. Urz. UE L 119 z 4.05.2016, s. 1 ze zmianą ogłoszoną w Dz. Urz. UE L 127 z 23.05.2018, s. 2. Dalej jako: „ogólne rozporządzenie o ochronie danych", „RODO" lub „rozporządzenie 2016/679".
[3] Dz. U. z 2019 poz. 1781.
[4] Dalej także jako „Prezes UODO".

Spis treści

Szanowni Państwo,

zgodnie z ustawą z 10 maja 2018 r. o ochronie danych osobowych, przedkładam Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności w roku 2019. Na mocy przepisu art. 59 ogólnego rozporządzenia o ochronie danych, sprawozdanie jest także udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

Niniejsze sprawozdanie przedstawia najważniejsze ustalenia z realizowanych przez Prezesa UODO ustawowych zadań, do których należą: rozpatrywanie skarg, prowadzenie kontroli, opiniowanie projektów aktów prawnych, przyjmowanie zgłoszeń naruszeń ochrony danych i podejmowanie czynności wobec administratorów i podmiotów przetwarzających w celu powiadomienia o naruszeniu osób, których dane dotyczą. Ważnym zadaniem jest również działalność edukacyjno-informacyjna oraz uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

W 2019 r. minął pełny rok kalendarzowy bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych w polskim porządku prawnym. To czas refleksji i podsumowań, jak w świetle prawa o ochronie danych podmioty różnych sektorów poradziły sobie z obsługą procesów przetwarzania danych osobowych w swoich organizacjach, oraz nad funkcjonowaniem Urzędu Ochrony Danych Osobowych – czy jego dotychczasowa struktura sprawdza się w praktyce pod kątem wymagań, jakie stawia RODO.

Zapraszam do lektury sprawozdania z działalności polskiego organu ochrony danych osobowych w roku 2019, które jest nie tylko rzetelną informacją o działalności polskiego organu nadzorczego, ale również podstawą do podejmowania decyzji służących zwiększeniu poziomu bezpieczeństwa danych osobowych obywateli.

Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

I. WPROWADZENIE

1. Źródła prawa w zakresie ochrony danych osobowych

Podstawę prawną działania Prezesa Urzędu Ochrony Danych Osobowych 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, wymagała 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], zaś w życie weszła 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].

---

[5] Dz. U. 2019, poz. 164
[6] Dz. U. 2019, poz. 697
[7] Dz. Urz. UE L 119 z 04.05.2016, s. 89 – dalej jako dyrektywa 2016/680 lub dyrektywa policyjna.
[8] Dz. U. z 2019 r. poz. 125
[9] Zgodnie z art. 18 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości jej art. 58 pkt 12 wszedł w życie 1 listopada 2019 r. Art. 82 pkt 5 w zakresie art. 25c–25h wszedł w życie 23 stycznia 2020 r.
[10] Dz. U. poz. 1041, rozporządzenie weszło w życie 6 czerwca 2019 r.

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 stosowania 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].

Na mocy art. 34 ust. 1 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych. Zgodnie z art. 34 ust. 2 przywołanej ustawy, Prezes UODO jest organem nadzorczym w rozumieniu:

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

Zgodnie z art. 57 RODO do zadań Prezesa UODO należy:

1. monitorowanie i egzekwowanie stosowania RODO;
2. 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);
3. 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;
4. upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO;

[11] tj. Dz. U. z 2016 r. poz. 922 z późn. zm.
[12] Wskazane przepisy obowiązywały do 5 lutego 2019 r.
[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. s. 53) – dalej jako: rozporządzenie 2016/794.

5. udzielanie osobom, których dane dotyczą, na ich żądanie, informacji o wykonywaniu praw przysługujących im na mocy RODO, a w stosownym przypadku współpraca w tym celu z organami nadzorczymi innych państw członkowskich UE;
6. 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;
7. współpraca z innymi organami nadzorczymi, w tym dzielenie się informacjami oraz świadczenie wzajemnej pomocy, w celu zapewnienia spójnego stosowania i egzekwowania RODO;
8. prowadzenie postępowań w sprawie stosowania RODO, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
9. 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;
10. przyjmowanie standardowych klauzul umownych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d RODO;
11. ustanowienie i prowadzenie wykazu operacji podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4 RODO;
12. udzielanie zaleceń, o których mowa w art. 36 ust. 2 RODO, dotyczących planowanych operacji przetwarzania danych;
13. 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;
14. 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;
15. gdy ma to zastosowanie — zgodnie z art. 42 ust. 7 RODO — dokonywanie okresowego przeglądu udzielonych certyfikacji;
16. opracowywanie i publikacja wymogów akredytacji podmiotów monitorujących kodeksy postępowania na mocy art. 41 oraz podmiotów certyfikujących na mocy art. 43;

17. akredytacja podmiotów monitorujących kodeksy postępowania zgodnie z art. 41 oraz podmiotów certyfikujących na mocy art. 43;
18. wydawanie zezwoleń na klauzule umowne i uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 RODO;
19. zatwierdzanie wiążących reguł korporacyjnych na mocy art. 47 RODO;
20. udział w pracach Europejskiej Rady Ochrony Danych;
21. prowadzenie wewnętrznego rejestru naruszeń ogólnego rozporządzenia o ochronie danych i działań podjętych zgodnie z art. 58 ust. 2 RODO;
22. wypełnianie innych zadań związanych z ochroną danych.

Wraz z powyższymi zadaniami, Prezesowi UODO przysługuje wiele uprawnień. **Należą do nich m.in. uprawnienia w zakresie prowadzonych postępowań przyznane na mocy art. 58 ust. 1 ogólnego rozporządzenia o ochronie danych.** Uprawnienia te obejmują:

1. nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;
2. prowadzenie postępowań w formie audytów ochrony danych;
3. dokonywanie przeglądu udzielonych certyfikacji na mocy art. 42 ust. 7 RODO;
4. zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia RODO;
5. uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;
6. 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 art. 58 ust. 2 ogólnego rozporządzenia o ochronie danych zalicza się:

1. wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu, dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
2. udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania;

3. nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO;
4. nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazanie sposobu i terminu;
5. nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
6. wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
7. 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;
8. 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;
9. 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;
10. 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 art. 58 ust. 3 RODO obejmują:

1. udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 36 RODO;
2. 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;
3. zezwalanie na przetwarzanie zgodnie z art. 36 ust. 5 RODO, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;
4. opiniowanie i zatwierdzanie projektów kodeksów postępowania zgodnie z art. 40 ust. 5 RODO;
5. akredytowanie podmiotów certyfikujących, w oparciu o przepis art. 43 RODO;
6. udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5;

7. przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d) RODO;
8. zezwalanie na klauzule umowne, o których mowa w art. 46 ust. 3 lit. a) RODO;
9. zezwalanie na uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b) RODO;
10. 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 z innych przepisów europejskich i krajowych. Na system ochrony danych osobowych składają się także 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.

Wobec rozpoczęcia obowiązywania od 25 maja 2018 r. ogólnego rozporządzenia o ochronie danych oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych[14], zasadniczej zmianie uległ dotychczasowy sposób podejścia do ochrony danych osobowych. Nowe regulacje spowodowały konieczność samodzielnej oceny przez administratorów ryzyka wiążącego się z przetwarzaniem danych osobowych dla praw i wolności osób, których dane dotyczą oraz wdrożenia przez te podmioty odpowiednich środków technicznych i organizacyjnych odpowiadających zidentyfikowanym ryzykom w taki sposób, aby możliwa była ich minimalizacja. Analiza spraw, którymi Prezes UODO zajmował się w okresie analizowanego roku sprawozdawczego, w tym w szczególności zgłaszanych skarg i pytań prawnych oraz naruszeń, które wpływały do organu w wyniku zgłoszeń dokonywanych przez administratorów, pozwoliło na zidentyfikowanie problemów związanych z ochroną danych osobowych, w związku ze stosowaniem RODO – problemów, które najczęściej pojawiały się zarówno po stronie podmiotów danych, jak i administratorów.

2. Urząd Ochrony Danych Osobowych

W wyniku wskazanej wyżej zmiany przepisów o ochronie danych w polskim systemie prawnym, nastąpiła także zmiana instytucjonalna. Na podstawie art. 167 ust. 1 ustawy o ochronie

[14] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 125).

danych osobowych Biuro Generalnego Inspektora Ochrony Danych Osobowych stało się Urzędem Ochrony Danych Osobowych (UODO). W strukturach Urzędu powstały Zespoły odpowiadające za realizację zadań wynikających z przepisów o ochronie danych osobowych dotyczących określonych sektorów.

Statutowe komórki organizacyjne Urzędu Ochrony Danych Osobowych nosiły następujące nazwy: Zespół Analiz i Strategii (ZAS), Zespół ds. Sektora Publicznego (ZSPU), Zespół ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa (ZSZZS), Zespół ds. Sektora organów Ścigania i Sądów (ZSOŚS), Zespół Wstępnej Oceny Skarg (ZWOS), Zespół ds. Sektora Prywatnego (ZSPR), Zespół Współpracy Międzynarodowej i Edukacji (ZWME), Zespół Współpracy z Administratorami Danych (ZWAD), Zespół Organizacyjny (ZO), Zespół ds. Kar i Egzekucji (ZKE), Zespół ds. Certyfikacji i Monitorowania Kodeksów (ZCMK), Zespół Prasowy, Zespół Informatyków, Zespół Administracyjny, Zespół Radców Prawnych, Dział Kontroli Wewnętrznej i Zarządczej, Dział Finansowy, Dział Kadr, Samodzielne Stanowisko Inspektora Ochrony Danych oraz Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych.

Zespoły realizowały kompetencje Prezesa UODO w zakresie m.in. rozpatrywania skarg na przetwarzanie danych osobowych, kierowanych przez osoby, których dane dotyczą, prowadzenia kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, opiniowania projektów aktów prawnych, udzielania odpowiedzi na pytania prawne, weryfikacji naruszeń zgłaszanych przez administratorów, a także prowadziły działalność edukacyjną, zmierzającą do poprawy ochrony danych osobowych we właściwych danemu Zespołowi sektorach.

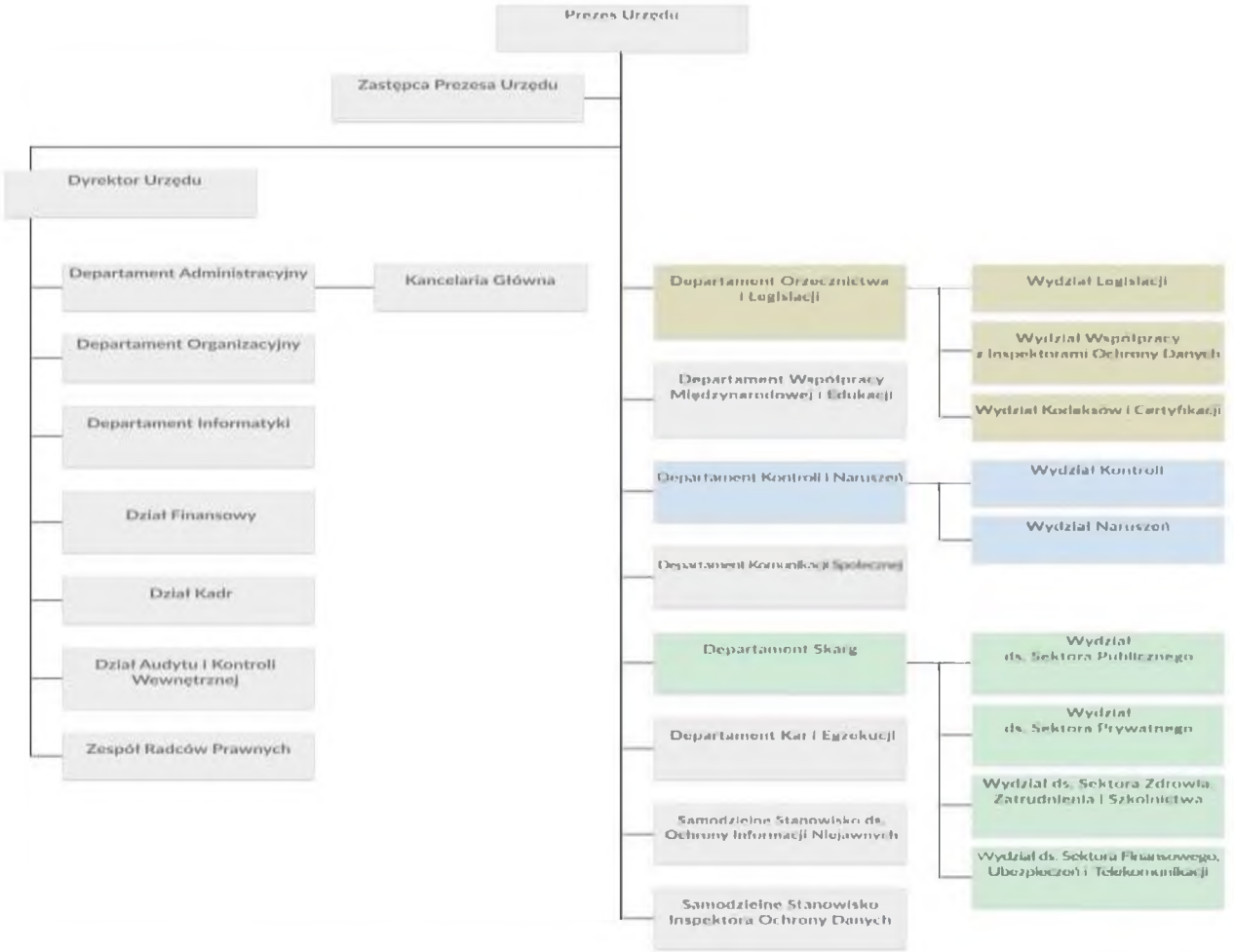
Wspomniane Zespoły funkcjonowały w strukturze organizacyjnej UODO do 30 listopada 2019 r. W tym czasie dokonano przeglądu funkcjonowania Urzędu w celu sprawdzenia, jak dotychczasowa struktura sprawdziła się w praktyce pod kątem wymagań stawianych przez RODO. Od 1 grudnia 2019 r. w miejsce dotychczasowych Zespołów tematycznych zostały utworzone nowe departamenty. Dla przykładu **skargi** są teraz w kompetencji jednego departamentu, **a kontrolami i naruszeniami czy orzecznictwem i legislacją** – zajmują się inne. W wymienionych departamentach wyodrębnione zostały **wydziały**, które zajmą się sprawami z określonych sektorów. I tak, w Departamencie Orzecznictwa i Legislacji powstały trzy wydziały: Legislacji, Współpracy z Inspektorami Ochrony Danych oraz Kodeksów i Certyfikacji. W Departamencie Kontroli i Naruszeń mamy obecnie Wydział Kontroli i Wydział Naruszeń, natomiast w Departamencie Skarg – Wydział ds. Sektora Publicznego, Wydział ds. Sektora Prywatnego, Wydział ds. Zdrowia, Zatrudnienia i Szkolnictwa oraz Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji.

Wdrożone zmiany pozwolą reagować na naruszenia ochrony danych osobowych bez uszczerbku dla realizowanych innych zadań organu. Usprawni to działania Urzędu i przełoży się na lepszą ochronę danych osobowych obywateli.

2.1. Struktura organizacyjna

UODO zapewnia wykonanie zadań wynikających z kompetencji Prezesa Urzędu Ochrony Danych Osobowych 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 19/2019 Prezesa UODO z 6 listopada 2019 r. w sprawie nadania statutu Urzędowi Ochrony Danych Osobowych[15].



[15] Opublikowany 29 listopada 2019 r. na stronie internetowej UODO, zob. link: https://uodo.gov.pl/pl/p/statut-urzedu.

2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2019 r. w przeliczeniu na pełne etaty wynosił 231,25 etatu (tj. 234 osoby). Natomiast zatrudnienie w UODO na dzień 31 grudnia 2019 r. wynosiło 243,05 etatu (tj. 246 osób). Na koniec 2019 r. na stanowiskach merytorycznych zatrudnionych było 216 osób, a na stanowiskach pomocniczych 30 osób. Wyższe wykształcenie posiadało 225 pracowników, w tym 133 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2019 r. przedstawiała się następująco:

1) Prezes UODO – 1 osoba,
2) Zastępca Prezesa UODO – 1 osoba,
3) Dyrektor Urzędu – 1 osoba,
4) Departament Orzecznictwa i Legislacji – 25 osób, w tym:
   - Wydział Legislacji – 10 osób,
   - Wydział Współpracy z Inspektorami Ochrony Danych – 4 osoby,
   - Wydział Kodeksów i Certyfikacji – 4 osoby,
5) Departament Współpracy Międzynarodowej i Edukacji – 14 osób,
6) Departament Kontroli i Naruszeń – 44 osoby, w tym:
   - Wydział Kontroli – 17 osób,
   - Wydział Naruszeń – 22 osoby,
7) Departament Komunikacji Społecznej – 14 osób,
8) Departament Skarg – 82 osoby, w tym:
   - Wydział ds. Sektora Publicznego – 15 osób,
   - Wydział ds. Sektora Prywatnego – 26 osób,
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 17 osób,
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 15 osób,
9) Departament Kar i Egzekucji – 8 osób,
10) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 1 osoba,
11) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba,
12) Departament Administracyjny – 24 osoby,
13) Departament Organizacyjny – 7 osób,
14) Departament Informatyki – 10 osób,

15) Dział Finansowy – 5 osób,
16) Dział Kadr – 4 osoby,
17) Dział Audytu i Kontroli Wewnętrznej – 1 osoba,
18) Zespół Radców Prawnych – 3 osoby,
19) Radca – samodzielne stanowisko – 2 osoby.

2.3. Budżet Urzędu Ochrony Danych Osobowych za 2019 r.

Budżet UODO ustalony w ustawie budżetowej na 2019 r. wynosił: 31 985 tys. zł, w tym:

- wynagrodzenia 21 441 tys. zł
- pochodne od wynagrodzeń 3 814 tys. zł
- wydatki majątkowe 70 tys. zł
- pozostałe wydatki 6 660 tys. zł

Wydatki zrealizowane przez UODO w 2019 r. w kwocie 31 390 tys. zł, w tym:

- wynagrodzenia 20 965 tys. zł
- pochodne od wynagrodzeń 3 778 tys. zł
- wydatki majątkowe 65 tys. zł
- pozostałe wydatki 6 582 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[16].

Dane osobowe dzielą się na trzy kategorie:

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**);

[16] 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.

- 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 podwaliną nowego prawa ochrony danych w UE. Rozporządzenie 2016/679 opiera się na podstawowych wartościach tego 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 do 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. Zadania jednostek organizacyjnych UODO

Do zadań jednostek organizacyjnych Urzędu Ochrony Danych Osobowych należy w szczególności: rozpatrywanie skarg w sprawach wykonania przepisów rozporządzenia 2016/679 i prowadzenie w tym zakresie postępowań administracyjnych, podejmowanie czynności w sprawie zgłaszanych przez administratorów naruszeń ochrony danych osobowych, prowadzenie postępowań w ramach współpracy i wzajemnej pomocy z organami nadzorczymi państw członkowskich, sporządzanie projektów pism procesowych w toku postępowań przed sądami oraz w toku innych postępowań, przedstawianie sądom poglądów w sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, opiniowanie projektów aktów prawnych dotyczących ochrony danych osobowych, w tym udział w konferencjach uzgodnieniowych w związku

z rozpatrywaniem projektów aktów prawnych w zakresie ochrony danych osobowych danego sektora (np. prywatnego, publicznego, zdrowia, zatrudnienia i szkolnictwa, organów ścigania i sądów), wydawanie opinii i stanowisk oraz kierowanie wystąpień o podjęcie działań zmierzających do wyeliminowania nieprawidłowości w procesach przetwarzania danych osobowych przez podmioty określonego sektora, a także opiniowanie projektów kodeksów postępowań przedkładanych do organu nadzorczego na mocy art. 42 rozporządzenia 2016/679 przez branże różnych sektorów.

Poszczególne jednostki organizacyjne UODO prowadzą działania kontrolne: sporządzają projekty rocznych i miesięcznych planów kontroli, których efektem, po zatwierdzeniu przez Prezesa UODO, było prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych. Przeprowadzane czynności kontrolne podsumowywane były w odpowiednich protokołach kontroli oraz pismach dokumentujących poszczególne czynności kontrolne. W razie stwierdzenia uchybień prowadzone były postępowania administracyjne w takich sprawach, a ich skutkiem było występowanie do Prezesa UODO o zastosowanie odpowiednich środków w celu przywrócenia stanu zgodnego z prawem, w przypadku stwierdzenia w wyniku kontroli naruszenia przepisów o ochronie danych osobowych, w tym nakładanie administracyjnych kar pieniężnych.

Ważnym zadaniem nałożonym na organ nadzorczy przepisami ogólnego rozporządzenia jest także realizacja obowiązków i uprawnień przez administratorów i inspektorów ochrony danych. Zadania te polegały m.in. na przyjmowaniu zawiadomień o wyznaczeniu inspektora ochrony danych (IOD), udzielaniu odpowiedzi na pytania od inspektorów ochrony danych oraz udzielaniu odpowiedzi na pytania od administratorów i podmiotów przetwarzających, przygotowaniu wystąpień w sprawach dotyczących statusu i zadań inspektorów ochrony danych oraz podejmowaniu działań informacyjno-edukacyjnych, przyczyniających się do budowania świadomości prawnej w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych. Ważnym zadaniem jest także przyjmowanie wniosków o uprzednie konsultacje, a także zgłoszeń naruszeń ochrony danych osobowych i podejmowanie czynności wobec administratorów i podmiotów przetwarzających w celu powiadomienia o naruszeniu osób, których dane dotyczą.

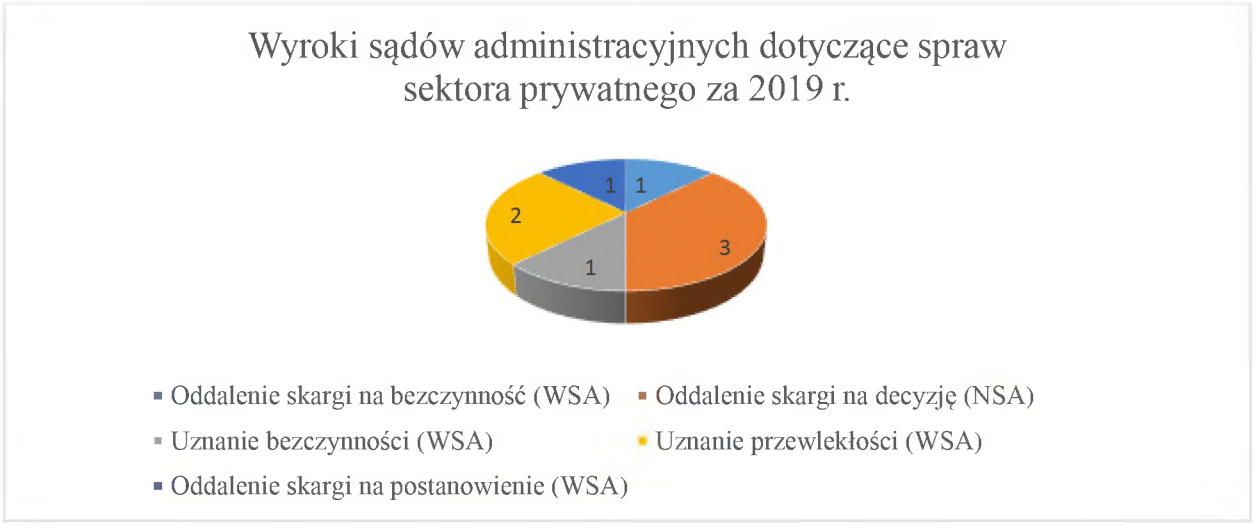
Art. 57 RODO wskazuje także na inne ważne zadanie organu nadzorczego – upowszechnianie i podnoszenie w społeczeństwie wiedzy z zakresu ochrony danych osobowych. Realizacja tego zadania została również ujęta w obowiązkach spoczywających na jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych.

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

W 2019 r. wniesiono do Wojewódzkiego Sądu Administracyjnego w Warszawie **89 skarg na decyzje lub postanowienia Prezesa UODO, z czego 23 skargi do WSA dotyczyły spraw sektora prywatnego, 14 – sektora publicznego, 35 – na decyzje wydane wobec podmiotów odpowiedzialnych za bezpieczeństwo publiczne i ściganie sprawców czynów zabronionych, 3 skargi na decyzje odmawiające udostępnienia informacji w trybie ustawy o dostępie do informacji publicznej oraz 14 – dotyczących czynności organu na etapie wstępnej oceny skarg.**

Dla porównania – w 2018 r. skarg na decyzje lub postanowienia Prezesa UODO było 77.

W 2019 roku na decyzje wydane wobec podmiotów sektora publicznego, do sądów administracyjnych skierowanych zostało **14 skarg**, w tym 1 na bezczynność. Natomiast w sprawach dotyczących podmiotów sektora prywatnego były to **23 skargi** (22 skargi do WSA na decyzje organu i 1 skarga na postanowienie wydane przez Prezesa UODO). W sprawach tych sądy administracyjne wydały 8 wyroków, co przedstawia poniższy *Wykres 1*.



Wykres 1: Wyroki sądów administracyjnych dotyczące spraw sektora prywatnego, wydanych przez organ nadzorczy w 2019 r.

W 2019 r. żadna z decyzji wydanych w sprawach dot. podmiotów sektora prywatnego nie została uchylona wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie. Wszystkie wyroki, które nie były oddaleniem skarg albo ich odrzuceniem, dotyczyły wyłącznie kwestii formalnych, takich jak przewlekłość prowadzonego postępowania oraz bezczynność organu.

Natomiast na decyzje Prezesa UODO w sprawach sektora organów ścigania i sądów, wpłynęło **35 skarg do Wojewódzkiego Sądu Administracyjnego w Warszawie** i w tych sprawach wydanych zostało **19 orzeczeń** przez sąd administracyjny. Stosownie do brzmienia art. 54 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi[17], skargi te – po ich przeanalizowaniu przez Prezesa UODO – były przekazywane wraz z odpowiedzią do Wojewódzkiego Sądu Administracyjnego w Warszawie (WSA) w terminie 30 dni od ich otrzymania. We wszystkich przypadkach skarg, Prezes UODO wniósł do WSA o ich oddalenie.

Jedna ze skarg do WSA dotyczyła decyzji Prezesa UODO, umarzającej postępowanie i wydanej w związku z zarzutami skarżącego wobec sądu w postępowaniu cywilnym. Skarżący zarzucił sądowi rejonowemu bezprawne przetwarzanie jego danych osobowych w prowadzonym przez ten sąd postępowaniu, polegające na przechowywaniu w aktach sprawy wydruku ze strony internetowej zawierającej informacje na temat działalności zawodowej skarżącego, w tym jego wizerunek. Wydruk ten stanowił załącznik do pisma procesowego jednej ze stron postępowania sądowego. Skarżący domagał się od Prezesa UODO wydania decyzji nakazującej usunięcie jego danych osobowych poprzez zniszczenie wydruku ww. strony internetowej z wizerunkiem skarżącego. Prezes UODO, wydając decyzję umarzającą w sprawie uzasadnił ją brakiem właściwości do wydania rozstrzygającej merytorycznie decyzji. Powołał się przy tym na brzmienie art. 55 ust. 3 RODO, zgodnie z którym organy nadzorcze nie mają właściwości rzeczowej do rozpatrywania spraw dotyczących przetwarzania danych w ramach czynności związanych ze sprawowaniem przez sądy wymiaru sprawiedliwości. Kwestię decydowania o treści i rodzaju dokumentów, które figurują w aktach prowadzonych spraw sądowych, Prezes UODO uznał za immanentnie powiązaną ze sprawowaniem wymiaru sprawiedliwości, w rezultacie czego orzekł o umorzeniu sprawy ze względu na jego bezprzedmiotowość. WSA, po rozpoznaniu sprawy ze skargi, orzekł o oddaleniu skargi, przychylając się tym samym do argumentacji przywołanej przez Prezesa UODO w zaskarżonej decyzji.

[17] Dz. U. z 2018 r. poz. 1302 z późn. zm.

Kolejna skarga na decyzję Prezesa UODO również dotyczyła przetwarzania danych osobowych przez sąd w związku z wchodzeniem interesantów do budynku sądu i pozyskiwane tych danych na podstawie dokumentów tożsamości. Skarżący podniósł, że praktyka taka nie ma podstaw w przepisach prawa i domagał się usunięcia jego danych z rejestru wejść do budynku sądu oraz zobowiązania prezesa sądu do zaniechania dalszego pozyskiwania i przechowywania danych osobowych interesantów. W decyzji wydanej w opisywanej sprawie Prezes UODO odmówił uwzględnienia wniosku skarżącego. W jej uzasadnieniu wskazał przede wszystkim, że przetwarzanie danych osobowych w elektronicznej księdze wejść sądu jest zgodne z przepisami prawa, w tym między innymi z dyspozycją art. 4 ust. 2 ustawy z dnia 6 kwietnia 1990 r. o Policji[18] oraz z ustawowo określonym zakresem zadań Policji, wśród których należy wymienić ochronę bezpieczeństwa i porządku publicznego w budynkach sądów i prokuratur. Z wyżej wymienionych powodów Prezes UODO uznał, że sąd z pomocą upoważnionych funkcjonariuszy Policji ma prawo przetwarzać dane osobowe interesantów wchodzących do budynku sądu, w tym także poprzez legitymowanie, skanowanie dokumentów i zapisywanie ich na nośnikach danych elektronicznych. WSA, po rozpatrzeniu skargi, przychylił się do argumentacji Prezesa UODO także w tym przypadku i orzekł o jej oddaleniu.

Należy wskazać, że wydane przez WSA w Warszawie orzeczenia w zakresie stwierdzenia bezczynności organu, wiązały się z szerszym problemem dotyczącym ograniczonych zasobów ludzkich Urzędu Ochrony Danych Osobowych i dużej rotacji pracowników, co znacząco utrudniało w pełni efektywne wykonywanie powierzonych zadań.

4. Wydawanie decyzji administracyjnych i rozpatrywanie skarg

Postępowanie dotyczące naruszenia przepisów o ochronie danych osobowych, wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej, toczy się według przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[19]. W przypadku stwierdzenia naruszenia przepisów prawa, postępowanie to może zakończyć się wydaniem decyzji administracyjnej, mocą której Prezes Urzędu Ochrony Danych Osobowych m.in.: umarza postępowanie, odmawia uwzględnienia wniosku skarżącego, nakazuje przywrócenie stanu zgodnego z prawem, nakłada karę, upomnienie albo ostrzeżenie na

[18] Dz. U. z 2019 r. poz. 161
[19] tj. Dz. U. z 2018 r. poz. 2096 z późn. zm., dalej jako: k.p.a.

administratora czy podmiot przetwarzający. Pomimo autonomii proceduralnej państw członkowskich UE pewne kwestie proceduralne, zwłaszcza związane z postępowaniami transgranicznymi, zostały bezpośrednio uregulowane w RODO.

Zgodnie z przepisami art. 35 § 3 k.p.a. organ ma miesiąc na załatwienie sprawy wymagającej postępowania wyjaśniającego, a w przypadkach szczególnie skomplikowanych termin ten wynosi dwa miesiące. Przestrzeganie tych terminów, zarówno w sprawach sprzed 25 maja 2018 r., jak i sprawach wszczętych po tym terminie, jest jednak trudne do skutecznej realizacji. Na wydłużenie czasu postępowań wpływa stopień skomplikowania oraz indywidualny charakter każdej sprawy, konieczność uzyskania wyczerpujących wyjaśnień, tak by zebrać stosowny materiał dowodowy w sprawie, będący podstawą wydania rozstrzygnięcia oraz uwzględnienia wszystkich aspektów sprawy. Dla długości prowadzonego postępowania mają także znaczenie kwestie związane z mniej lub bardziej udaną współpracą z administratorami i skarżącymi. W sytuacji, kiedy termin postępowania ulega przedłużeniu, organ informuje strony o tym fakcie oraz podaje orientacyjny okres przedłużenia wraz z terminem zakończenia sprawy.

Istotnym z punktu widzenia terminów rozpatrywania spraw jest fakt, że w dniu 5 listopada 2019 r. Wojewódzki Sąd Administracyjny rozpatrując skargę na bezczynność Prezesa UODO wydał wyrok w sprawie II Sa/Wa 634/19, w którym wziął pod uwagę przy uwzględnianiu terminów do rozpatrzenia sprawy, przepis art. 78 ust. 2 rozporządzenia 2016/679[20]. Sąd wydając niniejsze orzeczenie przyznał, że Prezes UODO rozpoznając postępowania może powoływać się na trzymiesięczny termin do dokonania czynności w sprawie. Sąd wskazał, że bezczynność organu administracji publicznej, w rozumieniu art. 3 § 2 pkt 8 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi[21] – ma miejsce wówczas, gdy organ nie załatwił sprawy w terminie określonym w art. 35 k.p.a. lub w przepisach szczególnych, ani w terminie wskazanym zgodnie z art. 36 § 1 k.p.a. Przypomniał, że od dnia 25 maja 2018 r. w polskim porządku prawnym obowiązuje ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[22] oraz rozporządzenie 2016/679, które stosuje się bezpośrednio. Zgodnie z art. 7 ust. 1 ustawy o ochronie

[20] Powołany przepis stanowi, że bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i 56 rozporządzenia 2016/679 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77 rozporządzenia 2016/679.

[21] Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (tj. Dz. U. z 2018 r. poz. 1302).

[22] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm).

danych osobowych, w postępowaniach prowadzonych przez Prezesa UODO, stosuje się przepisy k.p.a. w sprawach nieuregulowanych w ustawie o ochronie danych osobowych.

W świetle tak nakreślonych ram prawnych, Sąd dokonał kontroli i uznał, że Prezes UODO nie pozostawał w bezczynności.

Prezes UODO w roku 2019 rozstrzygał w sprawach dotyczących przetwarzania danych osobowych w kwestiach, które wielokrotnie były już przedmiotem postępowań 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 nowym wyzwaniom, zarówno po stronie administratorów, jak i po stronie organu nadzoru. Jeśli chodzi o administratorów to w toku prowadzonych postępowań są oni zobowiązani – zgodnie z zasadą rozliczalności – wykazać swoje przygotowanie i stosowanie nowych przepisów. Natomiast organ stale zmierza się z koniecznością dokonywania interpretacji nowych przepisów o ochronie danych osobowych, zaś skarżący nieustannie wykazują duże zainteresowanie dochodzeniem swoich praw z zakresu ochrony danych osobowych. Oczekują oni 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, art. 14 oraz 15 rozporządzenia 2016/679. Skarżący chcą także – często nie podejmując w pierwszej kolejności stosownych działań przed administratorem – aby organ nadzorczy wyręczył ich w realizacji ich praw z art. 15-22 rozporządzenia 2016/679. Takie żądania skarżący składają zwłaszcza, gdy kontakt z administratorem jest dla nich utrudniony.

Każda ze skarg analizowana jest pod kątem spełnienia warunków formalnych przewidzianych przepisami k.p.a. W sytuacji, gdy skarga nie spełniała warunków wymaganych przez ww. przepisy prawa, organ ochrony danych wzywał wnioskodawcę do ich usunięcia w przepisanym do tego terminie. Podobnie jak w ubiegłym okresie sprawozdawczym 2018 roku, skarżący wciąż popełniają te same błędy w zakresie wymogów formalnych w składanych przez nich pismach. Najczęściej skarżący wzywani są do doprecyzowania żądania mieszczącego się w zakresie kompetencji przysługujących Prezesowi UODO, gdyż większość z nich wnosi m.in. o samo wszczęcie postępowania w sprawie, nie wskazując podjęcia jakich działań w sprawie domagają się od Prezesa UODO. Skarżący wnoszą o stwierdzenie, czy doszło do naruszenia ich prawa do ochrony danych osobowych, przeprowadzenie kontroli w stosunku do skarżonego podmiotu, o nałożenie administracyjnej kary pieniężnej oraz o ustalenie podmiotu, który dopuszcza się naruszenia ich prawa do ochrony danych osobowych, a także wypłaty odszkodowania/zadośćuczynienia. Ponadto wnioskodawcy wzywani są do wskazania pełnej nazwy oraz adresu siedziby albo imienia, nazwiska

oraz adresu skarżonego podmiotu oraz do wskazania swojego adresu poczty tradycyjnej, w szczególności, gdy podanie wnoszone jest przez skarżących za pomocą środków komunikacji elektronicznej (ePUAP), gdyż błędnie przyjmują, że samo podpisanie podania: kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, powinno pozwolić zindywidualizować ich jako strony postępowania. Skarżący zostają także zobligowani do przedstawienia bardziej precyzyjnego opisu stanu faktycznego sprawy m.in. w zakresie wskazania danych, których dotyczy naruszenie i określenia na czym ono polega. W przypadku spraw dotyczących naruszenia ochrony danych osobowych w Internecie, Skarżący wzywani są do podania administratorów i linków stron internetowych. Sprawy, w których nie zostały usunięte braki formalne, pozostawione były bez rozpoznania.

W 2019 roku Prezes Urzędu Ochrony Danych Osobowych wydał 1369 decyzji administracyjnych, tj. o 842 więcej w stosunku do roku 2018, w którym wydanych było 527 decyzji.

4.1. Skargi

W omawianym 2019 roku do organu nadzorczego wpłynęły **9304 skargi,** tj. o 3739 więcej w stosunku do roku 2018, w którym skarg tych odnotowano 5565. Podkreślenia wymaga fakt, że z chwilą rozpoczęcia stosowania przepisów RODO, w okresie siedmiu miesięcy, tj. **od 25.05.2018 r. do 31.12.2018 r. do Urzędu Ochrony Danych Osobowych wpłynęło 4550 skarg.**

Podobnie jak w roku 2018, również w analizowanym roku sprawozdawczym 2019, zakres tematyczny skarg pozostawał bardzo szeroki. Dotyczył on wszelkich aspektów przetwarzania danych osobowych, a także odnosił się do szerokiego kręgu podmiotów – zarówno z sektora prywatnego jak i publicznego. Niemniej jednak można wskazać te zagadnienia, które pozostają nadal aktualne:

- pozyskiwanie, w związku z prowadzoną działalnością, danych osobowych bez podstawy prawnej, lub w zakresie szerszym, niż przewidziany przepisami prawa;
- dopuszczalny zakres danych oraz przesłanek legalizujących wykorzystywanie danych przez pracodawców, w tym przekazywanie danych osobowych pracowników podmiotom zewnętrznym;
- wykorzystanie urządzeń rejestrujących zarówno przez osoby fizyczne, jak i monitoringu wizyjnego stosowanego przez różnego rodzaju podmioty;

- przekazywanie danych firmom windykacyjnym i do BIK[23] bez podstawy prawnej bądź w sposób nieprzejrzysty dla osób, których te dane dotyczą;
- niewłaściwe zabezpieczenia danych osobowych w placówkach medycznych, firmach kurierskich, placówkach handlowo - usługowych;
- przetwarzanie danych za pomocą monitoringu instalowanego w placówkach szkolnych, spółdzielniach mieszkaniowych, czy przez właścicieli domów jednorodzinnych;
- ujawnienie lub zagubienie danych osobowych przez m.in. Pocztę Polską i firmy kurierskie, w ramach prowadzonej przez te podmioty działalności;
- wykorzystywanie danych do celów marketingowych;
- utrwalanie i pozyskiwanie danych osobowych poprzez kopiowanie dokumentów tożsamości przez banki oraz operatorów telekomunikacyjnych bądź żądanie ich kopii;
- udostępnianie danych osobowych osobom i podmiotom nieuprawnionym;
- brak realizacji obowiązków informacyjnych z art. 13 i 14 RODO;
- brak reakcji administratora na żądanie osoby, której dane dotyczą – najczęściej związanej z żądaniami wniesionymi na podstawie art. 15, 16, 17 lub 21 RODO[24].

4.1.1. Sektor publiczny

Udostępnianie danych przez instytucje publiczne

Kwestią będącą częstym przedmiotem postępowań administracyjnych prowadzonych przez Prezesa Urzędu w 2019 r. było udostępnienie przez instytucje publiczne danych osobowych osobom trzecim bądź innym instytucjom. W tego rodzaju sprawach Prezes Urzędu każdorazowo wskazywał, iż takie działanie jest dopuszczalne jedynie w sytuacji spełnienia przez administratora przesłanek zawartych w art. 6 ust. 1 RODO. W jednej z tego rodzaju spraw[25] skarżąca podniosła, że dyrektor powiatowego urzędu pracy (PUP) udostępnił jej dane osobowe, bez podstawy prawnej, Rzecznikowi Dyscyplinarnemu Okręgowej Rady Adwokackiej. Skarżąca (adwokat) w wyniku prawomocnego wyroku sądu powszechnego została zobowiązana do zwrotu środków na rozpoczęcie działalności gospodarczej, uzyskanych uprzednio od starosty na podstawie umowy

[23] BIK – Biuro Informacji Kredytowej S.A. Instytucja utworzona i działająca na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.).

[24] art. 15 RODO – Prawo dostępu przysługujące osobie, której dane dotyczą; art. 16 RODO – prawo do sprostowania danych, art. 17 RODO – prawo do usunięcia danych (prawo do bycia zapomnianym), art. 21 RODO – prawo do sprzeciwu.

[25] ZSPU.440.814.2018

zawartej z powiatowym urzędem pracy. W toku postępowania egzekucyjnego skarżąca wielokrotnie w pismach kierowanych do dyrektora PUP formułowała określenia powszechnie uznawane za poniżające, obelżywe zarówno w stosunku do kierownika jednostki, jak i pracowników merytorycznie odpowiedzialnych za prowadzenie spraw skarżącej. Z tego powodu dyrektor PUP skierował do Okręgowej Rady Adwokackiej „Skargę na czynności adwokata". Rzecznik Dyscyplinarny po otrzymaniu tej skargi zwrócił się do dyrektora PUP o nadesłanie kserokopii dokumentacji wskazanej w przedmiotowej skardze. Dyrektor PUP przesłał do Rzecznika Dyscyplinarnego kserokopię: umowy w sprawie przyznania skarżącej, jako bezrobotnej, jednorazowych środków na podjęcie działalności gospodarczej (z aneksami), rozliczenie ww. środków, pismo w sprawie nieterminowego wydatkowania środków, wyroki sądów wymienione w skardze oraz skargę skarżącej do rady powiatu na działania dyrektora PUP i uchwałę rady powiatu w sprawie rozpatrzenia tej skargi. Prezes Urzędu w wydanej decyzji w tej sprawie uznał, iż działania dyrektora PUP, mimo że miały charakter zmiany celu przetwarzania, znajdowały uzasadnienie w przepisach prawa, w szczególności ustawy Prawo o adwokaturze[26] oraz ustawy Kodeks postępowania karnego[27].

Do Urzędu Ochrony Danych Osobowych wpływały także skargi[28] dotyczące udostępnienia danych przez organy publiczne w związku z wykonywaniem ich ustawowych zadań. W jednej ze spraw[29] skarżący wystąpił do Wojewódzkiego Inspektora Ochrony Środowiska (WIOŚ) z wnioskiem o udostępnienie informacji o środowisku i jego ochronie, dotyczących funkcjonowania spalarni odpadów medycznych i weterynaryjnych. Otrzymał od WIOŚ tylko częściową odpowiedź, gdyż WIOŚ nie był w posiadaniu wszystkich żądanych informacji. Podstawą do żądania udostępnienia tej informacji przez skarżącego była ustawa o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko[30]. WIOŚ, zwracając się o udostępnienie brakujących informacji do podmiotu, który mógł być w ich posiadaniu, posłużył się treścią wniosku skarżącego skierowanego do WIOŚ, udostępniając jednocześnie temu podmiotowi dane osobowe skarżącego w zakresie jego imienia, nazwiska oraz adresu e-mail. Prezes Urzędu uznał, że choć dla potrzeb rozpatrzenia wniosku skarżącego dotyczących funkcjonowania spalarni odpadów medycznych i weterynaryjnych

[26] Ustawa z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2019 r. poz. 1513 z późn. zm.).
[27] Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2018 r. poz. 1987 z późn. zm.).
[28] np. ZSPU.440.91.2018, ZSPU.440.57.2018.
[29] ZSPU.440.57.2018
[30] Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz. U. z 2018 r. poz. 2081 z późn. zm.).

konieczne było zasięgnięcie przez WIOŚ opinii tego podmiotu, to jednak dla pozyskania jego stanowiska nie było niezbędne udostępnienie danych osobowych skarżącego. Takie działanie administratora danych naruszało zasadę legalności oraz rzetelności (art. 5 ust. 1 lit. a RODO) oraz zasadę celowości (art. 5 ust. 1 lit. b RODO), jak również nie znajdowało oparcia w przepisach prawa.

Zakres danych ujawnianych w prowadzonej korespondencji

Przedmiotem oceny Prezesa Urzędu była skarga na działania syndyka masy upadłości w toku postępowania upadłościowego prowadzonego wobec nieprowadzącej działalności gospodarczej osoby fizycznej, która ogłosiła upadłość[31]. W toku całego postępowania upadłościowego syndyk zamieszczał na kopertach zawierających korespondencję w tej sprawie numer PESEL dłużnika (upadłego). Zdaniem syndyka, z chwilą obwieszczenia w Monitorze Sądowym i Gospodarczym postanowienia sądu o ogłoszeniu upadłości skarżącej, w treści którego została ona zidentyfikowana w szczególności poprzez numer PESEL, dane te stały się danymi powszechnymi i opublikowanymi dla publicznej wiadomości. Nie kwestionując potrzeby należytej identyfikacji dłużnika (upadłego) i możliwości posługiwania się danymi pozwalającymi na jego identyfikację w ramach czynności służących wykonywaniu przez syndyka jego obowiązków, Prezes Urzędu wskazał jednak, że nie ma podstaw prawnych do posługiwania się numerem PESEL dłużnika (upadłego) na kopertach z przesyłkami do niego adresowanymi. Działania tego rodzaju wiążą się z niedopuszczalnym i zbędnym z punktu widzenia realizacji obowiązków syndyka, ujawnianiem numeru PESEL dłużnika osobom postronnym. Prezes Urzędu zwrócił uwagę zarówno na brak podstawy prawnej dla zaskarżonych działań syndyka, jak również naruszenie przez niego jednej z podstawowych zasad przetwarzania danych, tj. reguły minimalizacji danych. Zasada ta wymaga ograniczenia zakresu przetwarzanych informacji do minimum niezbędnego w kontekście podejmowanych czynności. Mając na uwadze, że postępowanie upadłościowe w rozpoznawanej sprawie zostało już zakończone, a w konsekwencji syndyk zaprzestał już ww. praktyk, w ramach rozstrzygającej niniejszą sprawę decyzji, Prezes Urzędu skierował do syndyka upomnienie.

Przetwarzanie danych osobowych na stronach Biuletynu Informacji Publicznej

Aktualny na gruncie rozpatrywanych przez Prezesa Urzędu skarg pozostaje temat udostępniania danych osobowych na stronach Biuletynu Informacji Publicznej (BIP), prowadzonych przez instytucje publiczne.

[31] ZSPU.440.572.2018

Na podstawie art. 4 ust. 1 ustawy o dostępie do informacji publicznej[32] podmioty publiczne i inne wykonujące zadania publiczne zostały zobowiązane do udostępnienia informacji publicznej, w szczególności na stronach BIP. Publikowane informacje obejmują zarówno dokumenty urzędowe, jak i materiały audiowizualne i teleinformatyczne dokumentujące te posiedzenia[33]. Zgodnie z art. 5 ust. 2 przywołanej ustawy, prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

W decyzjach wydawanych w 2019 r. Prezes Urzędu wielokrotnie stwierdzał, iż przetwarzanie danych osobowych w BIP, podobnie jak i w innych przypadkach, powinno się odbywać zgodnie z zasadami określonymi w art. 5 RODO. Szczególną uwagę zwracał przy tym na zasadę ograniczonego przechowywania (art. 5 ust. 1 lit. e RODO)[34], zgodnie z którą dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby przez okres nie dłuższy niż niezbędny do zrealizowania zakładanego celu. O tym, jak długo dane mogą być przechowywane, decyduje cel ich przetwarzania[35]. W przypadku, gdy określone przepisy nie regulują okresu przetwarzania danych w określony sposób, to na administratorze ciąży obowiązek oceny, czy cele zostały osiągnięte, czy też nie i czy dane są mu nadal potrzebne[36]. Administrator, publikując dane osobowe na stronach BIP, powinien to robić w sposób dokładny i staranny. Powinien ponadto regularnie dokonywać przeglądu przetwarzanych zbiorów pod kątem usuwania zbędnych danych. Administrator odpowiedzialny za publikowanie treści w BIP jest zobowiązany do każdorazowego dokonania stosownej oceny zasadności upublicznienia danych osobowych konkretnej osoby oraz do określenia okresu ich retencji.

Przedmiotem innej skargi[37], która wpłynęła do Urzędu w roku 2019, było udostępnienie przez starostę na stronach internetowych BIP protokołów z posiedzeń komisji rewizyjnej bez dokonania pełnej anonimizacji. Zdaniem skarżącej, pozostawienie w treści protokołów informacji

---

[32] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2019 r. poz. 1429).
[33] Art. 7 ust. 1 ustawy o dostępie do informacji publicznej.
[34] por. decyzja w sprawie ZSPU.440.477.2019.
[35] por. P. Drobek, komentarz do art. 5 RODO [w]: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz.* Wolters Kluwer Polska, 2018.
[36] por. P. Fajgielski, komentarz do art. 5 RODO [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz.* Wolters Kluwer Polska, 2018.
[37] ZSPU.440.138.2019

o wykładanym przez nią przedmiocie w szkole, w której świadczy pracę, czy zawodzie jej męża umożliwia jej zidentyfikowanie. Po analizie sprawy Prezes Urzędu stwierdził, iż skarżąca jest osobą pełniącą funkcję publiczną w rozumieniu art. 5 ust. 2 ustawy o dostępie do informacji publicznej, a zamieszczone na stronie internetowej BIP starostwa dane osobowe mają związek ze sprawowaną przez nią funkcją. Prezes Urzędu stwierdził, że z tego względu w jej przypadku nie ma zastosowania ograniczenie udostępnienia informacji ze względu na prywatność osoby fizycznej.

Ochrona danych osobowych sygnalistów informujących organy publiczne o zaobserwowanych nieprawidłowościach

W 2019 r. do Prezesa UODO wpływało także wiele skarg[38] od osób, które sygnalizowały organom publicznym niezgodne z prawem działania innych podmiotów bądź osób.

W jednej z nich[39] skarżący zawiadomił Powiatowy Inspektorat Nadzoru Budowlanego (PINB), o podejrzeniu wykonania dróg gruntowych niezgodnie z przepisami ustawy Prawo budowlane[40]. Na skutek tego zawiadomienia PINB przeprowadził wobec burmistrza postępowanie kontrolne, które zakończyło się wydaniem decyzji administracyjnych, w treści których umieszczone zostały: imię, nazwisko skarżącego oraz informacje o otrzymanym od niego zawiadomieniu. W ocenie Prezesa Urzędu, takie udostępnienie danych skarżącego naruszyło zasadę legalności, rzetelności i celowości, jak również art. 6 ust. 1 RODO. W związku ze stwierdzonymi uchybieniami w przestrzeganiu przepisów RODO Prezes UODO udzielił PINB upomnienia.

Prezes Urzędu wielokrotnie w wydanych przez siebie decyzjach oraz wystąpieniach[41] podkreślał, iż przepisy Kodeksu postępowania administracyjnego[42] wyposażają organy administracji publicznej w instrumenty pozwalające na zbadanie sygnalizowanych przez mieszkańców nieprawidłowości bez ujawniania źródła informacji. Osoba zawiadamiająca o potencjalnych naruszeniach, ale nierobiąca tego ze względu na swój interes prawny lub obowiązek, nie powinna stać się jego stroną. Nieracjonalne i nieuzasadnione jest bowiem traktowanie jako strony każdego, kto informuje organ o zaobserwowanych uchybieniach. Przepisy k.p.a. (art. 61 § 1) umożliwiają organom administracji publicznej zbadanie tego typu sygnałów przez wszczęcie postępowania z urzędu. Wówczas (zgodnie z art. 28 k.p.a.) jego stroną staje się

[38] np.: ZSPU.440.339.2018, ZSPU.440.553.2018, ZSPU.440.740.2018.
[39] ZSPU.440.740.2018.
[40] Ustawa z dnia 7 lipca 1994 r. Prawo budowlane (Dz. U. z 2019 r. poz. 1186 z późn. zm.).
[41] ZSPU.440.339.2018.
[42] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2018 r. poz. 2096 z późn. zm.).

wyłącznie osoba, której stawiane są zarzuty, a nie osoba zawiadamiająca o możliwych naruszeniach. Ta ostatnia nie jest więc wprawdzie informowana o przebiegu postępowania oraz o jego wynikach, ale jednocześnie nie dochodzi do ujawniania jej danych osobowych, a przez to naruszenia jej prywatności.

O tym jak ważną rolę w społeczeństwie odgrywają osoby informujące o zaobserwowanych nieprawidłowościach świadczy zainteresowanie tym tematem organów unijnych i przyjęcie przez Parlament Europejski w dniu 16 kwietnia 2019 r. dyrektywy o ochronie osób zgłaszających przypadki naruszenia prawa Unii (tzw. dyrektywa o ochronie sygnalistów). Państwa członkowskie mają obowiązek implementować jej zapisy do krajowych porządków prawnych.

„Prawo do bycia zapomnianym" w sektorze publicznym

W 2019 r. do Urzędu Ochrony Danych Osobowych wpłynęła skarga[43] na przetwarzanie danych pozyskanych w związku z przeprowadzeniem postępowania sprawdzającego w trybie przepisów ustawy o ochronie informacji niejawnych[44].

Administrator zgodnie z art. 6 ust. 1 lit. c RODO jest uprawniony do przetwarzania danych osobowych w przypadku, gdy m.in. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Dane osobowe skarżącego zawarte w ankiecie bezpieczeństwa po ustaniu stosunku pracy podlegają obowiązkowi archiwizacji. Obowiązek ten został nałożony przepisami ustawy o ochronie informacji niejawnych. W opinii organu w sprawie zaszła okoliczność z art. 17 ust. 3 lit. b RODO wyłączająca uprawnienie skarżącego do żądania usunięcia jego danych osobowych zgromadzonych w aktach postępowania sprawdzającego. Nie stwierdzono również, aby administrator danych, w okresie od dnia ustania stosunku pracy skarżącego do dnia wydania decyzji umarzającej postępowanie sprawdzające, dokonywał jakichkolwiek operacji przetwarzania danych osobowych skarżącego zgromadzonych w aktach postępowania sprawdzającego, za wyjątkiem ich przechowywania. W analizowanej sprawie wykazano, iż realizacja „prawa do bycia zapomnianym" podlega określonym w przepisach RODO wyłączeniom. Z „prawa do bycia zapomnianym" nie może np. skorzystać osoba, której dane osobowe są przetwarzane w związku z koniecznością wywiązania się z prawnego obowiązku wymagającego przetwarzania z mocy przepisów prawa, któremu podlega administrator, lub gdy dane te są niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

---

[43] ZSPU.440.413.2018.

[44] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2109 r. poz. 742 z późn. zm.).

Wykorzystywanie danych z rejestrów publicznych

W 2019 r. do Urzędu wpłynęło również wiele skarg[45] od osób, których dane osobowe upublicznione zostały w Krajowym Rejestrze Sądowym (KRS), w związku z pełnieniem przez nich funkcji w organach spółek. Przedmiotem tych spraw było przetwarzanie danych osobowych tych osób w prywatnym serwisie internetowym, publikującym dane w oparciu o informacje ujawnione w KRS. Upubliczniane były takie dane, jak: imię, nazwisko, funkcja pełniona w organach spółki, a także liczba oraz wartość posiadanych udziałów w przypadku udziałowców. Prezes Urzędu stwierdził, iż ww. dane są danymi powszechnie dostępnymi, a ich zakres jest adekwatny w kontekście realizowanego przez właściciela serwisu celu informacyjnego. Należy zauważyć, iż opublikowane dane mają węższy zakres, niż dane ujawnione w KRS – nie obejmują bowiem numeru PESEL. Wykorzystanie danych osobowych pozyskanych z publicznego rejestru było przedmiotem rozpoznania przez Naczelny Sąd Administracyjny. Sąd ten wskazał m.in., iż celem rejestrów publicznie dostępnych jest udostępnienie informacji na potrzeby obrotu prawnego i aktualnie brak jest przepisów, które by nakazywały spełnienie obowiązków w zakresie pozyskiwania danych z publicznych rejestrów[46]. Przetwarzanie publicznie dostępnych danych osobowych osoby pełniącej określone funkcje w podmiotach podlegających wpisowi do rejestru (członka organu, wspólnika czy prokurenta), w tym ich publikacja, w ocenie Prezesa Urzędu znajduje oparcie w powołanym art. 6 ust. 1 lit. f RODO, tj. ze względu na prawnie uzasadniony interes realizowany przez administratora.

Na gruncie jednej z tego typu spraw[47] rozważaniom Prezesa Urzędu podlegała również kwestia wypełnienia obowiązku informacyjnego, o którym mowa w art. 14 RODO[48], przez podmiot publikujący dane osobowe pozyskane z KRS na swojej stronie internetowej. Wobec spoczywającego na administratorze obowiązku przestrzegania wyrażonej w art. 5 ust. 1 lit. c RODO reguły minimalizacji danych (obligującej go do ograniczenia zakresu przetwarzanych danych do niezbędnego, adekwatnego do realizowanego celu minimum), nie można zasadnie oczekiwać od podmiotu pozyskania i przetwarzania w celach informacyjnych (wyłącznie dla celu spełnienia obowiązku z art. 14 RODO), dalszych jego danych osobowych[49] (tj. danych adresowych). Prezes

[45] Np. ZSPU.440.105.2019, ZSPU.440.704.2018, ZSPU.440.705.2018, ZSPU.440.574.2018, ZSPU.440.684.2018.
[46] por. wyrok NSA z 3 grudnia 2015 r. sygn. akt I OSK 1166/14.
[47] ZSPU.440.574.2018
[48] Art. 14 ust. 1 RODO jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, informacje odpowiednio wskazane w art. 14 ust. 1 oraz ust. 2 RODO.
[49] por. wyrok NSA z 24 stycznia 2013 r. sygn. akt I OSK 1827/11, wyrok WSA w Warszawie z 28 kwietnia 2014 r. sygn. akt II SA/Wa 125/14.

Urzędu w analizowanej sprawie uznał, iż administrator spełnił warunki określone w art. 14 ust. 5 lit. b RODO[50]. Zamieszczenie przez administratora niezbędnych informacji na stronie internetowej stanowiło przedsięwzięcie odpowiednich i wystarczających środków w kontekście ochrony praw i wolności osoby, której dane dotyczą. W szczególności osoba ta uzyskała w ten sposób informację na temat procesu przetwarzania jej danych, administratora tych danych i możliwości kontaktu z nim oraz uprawnień związanych z dokonywanym przez niego przetwarzaniem danych. W konsekwencji w rozpoznawanej sprawie nie stwierdzono naruszenia art. 14 ust. 1 i 2 RODO – na skutek wyłączenia ich stosowania na mocy art. 14 ust. 5 lit. b RODO.

Reasumując, o ile dane osobowe przetwarzane w rejestrach publicznych mogą być legalnie pozyskiwane przez inne podmioty/osoby, to należy pamiętać, że przetwarzając (m.in. udostępniając, upubliczniając) te dane, jako ich administratorzy, podmioty te są zobowiązane do spełnienia obowiązków wynikających z przepisów RODO.

Prowadzenie postępowań egzekucyjnych przez komorników sądowych

Przedmiotem postępowań prowadzonych przez Prezesa Urzędu w 2019 r. były m.in. skargi na przetwarzanie danych w związku z prowadzonymi przez komorników sądowych postępowaniami egzekucyjnymi.

Należy zaznaczyć, iż obowiązujące przepisy prawa nie uprawniają Prezesa UODO do prowadzenia czynności nadzorczych nad wykonywanymi przez komornika sądowego czynnościami egzekucyjnymi. Prezes Urzędu nie może kontrolować postępowań prowadzonych przez inne organy, a w szczególności ingerować w określone ustawowo kompetencje innych organów, wkraczać w prowadzone w zakresie ich właściwości postępowania i dokonywać merytorycznej oceny poszczególnych czynności wykonywanych w ramach tych postępowań. Ma jedynie prawo badania kwestii związanych z przetwarzaniem danych osobowych.

W jednej ze spraw[51] komornik, sugerując się jedynie wskazanym przez wierzyciela we wniosku numerem PESEL, błędnie zidentyfikował osobę dłużnika. Mimo iż komornik, zgodnie z przepisami kodeksu cywilnego[52], jest związany wnioskiem o wszczęcie egzekucji i po uzyskaniu

---

[50] Art. 14 ust. 5 lit. b RODO: udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie.

[51] ZSPU.440.296.2019

[52] Art. 804 ustawy dnia 17 listopada 1963 r. Kodeks postępowania cywilnego (Dz.U. z 2019 r. poz. 1460 z późn. zm.).

sprawy od wierzyciela nie ma obowiązku badać, czy rzeczywiście zachodzi podstawa do jej wszczęcia (zadanie to należy do sądu), to jednak zawsze bezwzględnie powinien sprawdzić poprawność informacji przekazanej przez wierzyciela, w tym dokonać weryfikacji tożsamości dłużnika. W tym przypadku wierzyciel podał komornikowi nieprawidłowy nr PESEL dłużnika. Jednak podał on także jego imię i nazwisko. Komornik, wprowadzając podany numer do systemu Pesel-Net, również pozyskał z niego imię, nazwisko oraz adres zamieszkania osoby posługującej się tym numerem identyfikacyjnym. Jego obowiązkiem było zaś zweryfikowanie zgodności tych danych z wnioskiem wierzyciela. W razie wątpliwości powinien zgłosić się do niego w celu ich wyjaśnienia. Komornik tego nie zrobił, w wyniku czego bezprawnie pozyskał dane osoby niebędącej dłużnikiem i dalej bezprawnie je przetwarzał dołączając je do akt prowadzonego postępowania egzekucyjnego, przez co nie było możliwości ich usunięcia. W wydanej decyzji Prezes UODO zaznaczył, że działania komornicze, takie jak zajęcie rachunku, wynagrodzenia za pracę czy licytacja majątku, szczególnie istotnie oddziałują na osobę, przeciwko której są skierowane i mają istotny wpływ na jej sytuację materialną, a w dalszej kolejności na inne sfery życia. Dlatego jednoznaczna i prawidłowa identyfikacja dłużnika jest kluczowym elementem każdego postępowania egzekucyjnego. Komornicy muszą pamiętać, że wykonują zawód zaufania publicznego i ciąży na nich szczególny obowiązek przestrzegania prawa i zachowania dokładności w dokonywanych czynnościach. W ocenie Prezesa Urzędu, działanie komornika w rozpatrywanej sprawie naruszyło art. 5 ust. 1 lit. d i f RODO, tj. zasadę prawidłowości i poufności przetwarzania danych, i związku z tym Prezes UODO udzielił mu upomnienia.

Przetwarzanie danych osobowych w sektorze mieszkalnictwa

W roku 2019 Prezes Urzędu badał legalność przetwarzania danych przez spółdzielnie mieszkaniowe[53]. W tych sprawach ocenie podlegała m.in. kwestia przetwarzania danych osób, które nie były członkami spółdzielni. Dokonano analizy przepisów ustawy o spółdzielniach mieszkaniowych[54] pod kątem zastosowania regulacji zawartej w art. 6 ust. 1 lit. c RODO, która czyni legalnym przetwarzanie danych przez administratora pod warunkiem istnienia odpowiedniej podstawy prawnej.

Treść art. 4 ustawy o spółdzielniach mieszkaniowych zawiera regulacje dotyczące obowiązku ponoszenia opłat związanych z eksploatacją i utrzymywaniem ich lokali oraz nieruchomości wspólnych. Przepis art. 4 ust. 4 tej ustawy stanowi, iż właściciele lokali niebędący członkami

[53] ZSPU.440.15.2018, ZSPU.440.13.2019, ZSPU.440.16.2019, ZSPU.440.17.2019.
[54] Ustawa z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2018 r. poz. 845).

spółdzielni są obowiązani uczestniczyć w pokrywaniu kosztów związanych z eksploatacją i utrzymaniem ich lokali, eksploatacją i utrzymaniem nieruchomości wspólnych oraz uczestniczyć w wydatkach związanych z eksploatacją i utrzymaniem nieruchomości stanowiących mienie spółdzielni, które są przeznaczone do wspólnego korzystania przez osoby zamieszkujące w określonych budynkach lub osiedlu. Obowiązki te wykonują przez uiszczanie opłat na takich samych zasadach, jak członkowie spółdzielni, z zastrzeżeniem art. 5. Z kolei zgodnie z art. 4 ust. 6 ustawy o spółdzielniach mieszkaniowych, za opłaty, o których mowa w ust. 1-2 i 4, odpowiadają solidarnie z członkami spółdzielni, właścicielami lokali niebędącymi członkami spółdzielni lub osobami niebędącymi członkami spółdzielni, którym przysługują spółdzielcze własnościowe prawa do lokali, osoby pełnoletnie stale z nimi zamieszkujące w lokalu, z wyjątkiem pełnoletnich zstępnych pozostających na ich utrzymaniu, a także osoby faktycznie korzystające z lokalu. Wyżej wymieniona ustawa, na co wskazuje treść cytowanych przepisów, zawiera uregulowania dotyczące osób niebędących członkami spółdzielni, nakładając na nich obowiązek ponoszenia opłat związanych z eksploatacją i utrzymywaniem ich lokali oraz nieruchomości wspólnych.

Prezes Urzędu uznał, iż ww. przepisy stanowią podstawę do przetwarzania przez spółdzielnie mieszkaniowe danych osobowych osób niebędących członkami spółdzielni, a jest to związane z realizacją przez spółdzielnię mieszkaniową zadań, obowiązków i uprawnień określonych w statucie, regulaminach spółdzielni czy wynikających z przepisów prawa związanych z prowadzeniem działalności zarządzania i administrowania nieruchomościami. Rola spółdzielni w tym zakresie polega w szczególności na prowadzeniu ewidencji opłat czy prowadzeniu rozliczeń z ww. osobami, co statuuje konieczność przetwarzania ich danych osobowych dla tych właśnie celów. Przetwarzanie danych odbywa się w oparciu o przepisy prawa, a przesłanką legalizującą takie działanie jest art. 6 ust. 1 lit. c RODO.

Przedmiotem innych spraw dotyczących przetwarzania danych przez wspólnoty mieszkaniowe najczęściej była też kwestia ich nieprawidłowego zabezpieczenia skutkującego udostępnieniem danych osobom do tego nieupoważnionym.

W jednej ze spraw[55] wspólnota mieszkaniowa korespondencję zawierającą dane osobowe dłużników wspólnoty mieszkaniowej (imię, nazwisko, adres zamieszkania oraz informację o kwocie zadłużenia) wrzuciła bez odpowiedniego zabezpieczenia do skrzynek pocztowych, co umożliwiło dostęp do treści w niej zawartych osobom nieuprawnionym, np. wynajmującym

[55] ZSPU.440.184.2019

mieszkania. Prezes Urzędu skierował w tej sprawie do wspólnoty mieszkaniowej wystąpienie z żądaniem wprowadzenia odpowiednich rozwiązań mających zapobiegać takim naruszeniom w przyszłości. Wskazał w nim, że zgodnie z art. 27 ustawy o własności lokali[56], prawo i obowiązek współdziałania w zarządzie nieruchomością wspólną, a więc również uzyskiwania informacji o zadłużeniach poszczególnych lokali, ma jedynie właściciel lokalu. Wspólnota mieszkaniowa powinna w taki sposób zorganizować doręczanie wszelkiej korespondencji zawierającej dane osobowe jej członków, aby skutecznie chronić je przed dostępem osób trzecich.

W innej sprawie[57] z kolei, korespondencja kierowana do członków wspólnoty mieszkaniowej była doręczana im przez osobę trzecią, nieposiadającą stosowanego upoważnienia do przetwarzania danych osobowych. Prezes Urzędu wskazał, iż administrator przetwarzając dane osobowe, w każdym wypadku jest zobowiązany do przestrzegania nałożonego na niego obowiązku związanego z zapewnieniem odpowiedniego zabezpieczenia przetwarzanych danych osobowych wynikającego z treści art. 32 RODO. Poprzez udostępnienie danych osobowych osobie nieuprawnionej administrator dopuścił się naruszenia zasady poufności i integralności wyrażonej w art. 5 ust. 1 lit. f RODO. Wobec zaistnienia ww. nieprawidłowości w procesie przetwarzania danych osobowych Prezes Urzędu skierował do administratora danych osobowych upomnienie, w którym wskazał na konieczność zaprzestania praktyk związanych z powierzaniem danych osobom nieuprawnionym.

4.1.2. Sektor prywatny

W 2019 r. duża część postępowań i skarg dotyczących sektora prywatnego dotyczyła wniosków o rzeczywistą wykładnię zasad przetwarzania danych osobowych oraz przesłanek legalizacyjnych, opisanych w art. 5 i 6 rozporządzenia 2016/679 – w odniesieniu do działalności podmiotów telekomunikacyjnych, podmiotów windykacyjnych, wpisów zawartych i zaindeksowanych w wyszukiwarkach internetowych, a także tzw. „giełdy długów", czy wywiadowni gospodarczych. Skarżący żądali ograniczenia zakresu przetwarzania ich danych osobowych (respektowania zasady minimalizacji danych) – w odniesieniu do kserowania dowodów osobistych w związku z zawarciem umów (bankowych, telekomunikacyjnych), w związku z przekazywaniem ich danych osobowych do firm windykacyjnych, bądź przekazaniem ich danych osobowych przez banki do podmiotów takich jak BIK, czy Bankowy Rejestr. Skarżący żądali nakazania zaprzestania przetwarzania ich danych osobowych przez podmioty w odniesieniu do

[56] ustawa z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. z 2019 r. poz. 737 z późn. zm.).
[57] ZSPU.440.207.2019

wpisów figurujących w rejestrach bankowych czy podmiotach takich jak BIK czy Bankowy Rejestr, albo też usunięcia ich danych z jawnych rejestrów (np. CEIDG), chcąc w ten sposób egzekwować prawo do bycia zapomnianym. Skarżący wnosili o ukaranie ww. podmiotów za przekroczenie przez nie uprawnień w zakresie przetwarzania danych osobowych osób fizycznych. Skarżący kwestionowali udzielone wcześniej zgody na przetwarzanie ich danych osobowych w celach realizacji umów, które zawierali z podmiotami (bankowe, telekomunikacyjne, ubezpieczeniowe). Żądali respektowania zasady rzeczywistej odwoływalności zgody, którą uprzednio wyrazili. Kwestionowali ponadto cele, w jakich podmioty przetwarzały ich dane osobowe w odniesieniu do prowadzonych działań marketingowych. Kwestionowali konieczność przetwarzania danych niezbędnych do wypełnienia obowiązków prawnych ciążących na administratorze oraz do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratorów lub przez stronę trzecią.

W toku prowadzonych postępowań weryfikowane były wszelkie żądania osób skarżących. I tak, już na etapie wpływu skargi, np. prawo do bycia zapomnianym nie mogło być respektowane w odniesieniu do wpisów dokonywanych w rejestrach państwowych czy zbiorach prowadzonych na podstawie przepisów prawa, lub w sytuacji legitymowania się uzasadnionym interesem prawnym. Prawo do bycia zapomnianym nie ma charakteru bezwzględnego. Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej, działają w granicach i zgodnie z przepisami prawa. Jeżeli otrzymane przez te organy publiczne dane osobowe są im niezbędne do przeprowadzenia określonego postępowania (np. postępowania upadłościowego, reklamacyjnego, egzekucyjnego) mającego podstawy w przepisach prawa, a zatem dane wykorzystane są do realizacji celu zgodnego z tymi przepisami, to nie doszło do ujawnienia i przetwarzania danych osobowych osoby fizycznej w sposób nieuzasadniony. Każdorazowo w toku prowadzonych postępowań uwzględniany i wyważany jest interes stron postępowania. Z oceny skarg, które w 2019 r. wpłynęły do Urzędu wynika, że w większości przypadków żądania skarżących sprowadzają się do kwestionowania obowiązujących przepisów prawa. W świetle powyższego UODO prowadził postępowania mające na celu realizację swoich obowiązków, a nadto podejmował działania informacyjne, respektując postanowienia wyrażone w rozporządzeniu 2016/679.

W ciągu półtora roku stosowania rozporządzenia 2016/679, tj. w okresie 25.05.2018 – 31.12.2019, dało się zauważyć kilka ciekawych tendencji w zakresie skarg. O ile, podobnie jak przed 25 maja 2018 r., porównywalnie liczne były skargi dotyczące prawa bankowego, windykacji długów czy kwestii przetwarzania danych osobowych w celach marketingowych, o tyle pojawił się

również cały szereg nowych zagadnień oraz spraw pokazujących wzrost świadomości prawnej społeczeństwa. Na znaczeniu zyskało wykonywanie obowiązku administracyjnego, uregulowane obecnie w art. 13, 14 oraz 15 RODO. Skarżący składają również wnioski o udostępnienie im kopii danych w trybie art. 15 ust. 3 rozporządzenia 2016/679, myląc to z obowiązkiem wydania im przez administratora dokumentów, które zawierają ich dane osobowe. Zdarzały się również liczne wnioski o udostępnienie nagrań z monitoringu wizyjnego prowadzonego w podmiotach takich jak, np. sklepy, centra handlowe, jak też wnioski o udostępnienie nagrań z infolinii w celu złożenia skutecznej reklamacji i udowodnienia okoliczności dotyczących, np. zakupu określonych produktów z wadami fabrycznymi, bądź też nienależytego wykonania polecenia wydanego drogą telefoniczną przez posiadacza rachunku przez pracownika banku w odniesieniu do konta bankowego klienta. Istotnymi podnoszonymi przez skarżących zagadnieniami były wnioski o przeprowadzenie kontroli w podmiotach prywatnych w zakresie monitoringu wizyjnego podmiotów użyteczności publicznej (przebieralnie na basenie).

Dużym zainteresowaniem cieszyło się również przysługujące na podstawie art. 17 rozporządzenia 2016/679 prawo do usunięcia danych, zwane też „prawem do bycia zapomnianym", w dużej części w zakresie postępowań windykacyjnych prowadzonych za pośrednictwem stron internetowych, jak i w odniesieniu do danych osób fizycznych publikowanych w wyszukiwarce internetowej Google. Skarżący traktowali to uprawnienie w sposób bezwzględny, co było daleko idącym uproszczeniem, ponieważ nie zawsze można było żądać usunięcia wszystkich swoich danych osobowych, zwłaszcza w sytuacji, gdy dane osobowe przetwarzane były zgodnie z prawem w wielu różnych celach. I tylko dlatego, że zakończył się jeden z celów przetwarzania, np. nastąpił koniec umowy, nie oznaczało to zaprzestania przetwarzania danych w ogóle, zgodnie z obowiązującymi przepisami prawa. Ponadto skarżący często powoływali się na zasady przetwarzania danych osobowych opisywane w art. 5 rozporządzenia 2016/679, ze szczególnym uwzględnieniem zasady minimalizacji danych, ograniczenia celu oraz integralności i poufności danych.

Windykacja

W 2019 r. utrzymał się trend składania skarg na przetwarzanie danych osobowych związane z dochodzeniem roszczeń od dłużników. W postępowaniach przed organem dłużnicy najczęściej kwestionowali zasadność roszczenia, wskazywali na brak ich zgody na przetwarzanie danych osobowych przez wierzyciela oraz wyrażali żądanie usunięcia ich danych przetwarzanych, w ich opinii, bez podstawy prawnej. Kolejnym ważnym czynnikiem, który wpływał na ilość skarg w tej

grupie było kwestionowanie przez dłużników legalności cesji wierzytelności bez ich zgody. W skargach powtarzało się także kwestionowanie legalności powierzenia osobom trzecim danych osobowych dłużników przez fundusze sekurytyzacyjne lub innych wierzycieli, w celu dochodzenia wierzytelności. Firmom windykacyjnym zarzucane było także omyłkowe występowanie z roszczeniami wobec osób trzecich, wskutek pomyłki w identyfikacji dłużnika (identyczne imię, nazwisko i miasto zamieszkania) lub wskutek kradzieży tożsamości. Dłużnicy często podnosili brak spełnienia wobec nich obowiązku informacyjnego, wynikającego z art. 14 rozporządzenia 2016/679, zarówno przez wierzyciela (administratora), jak i przez podmioty trzecie, którym wierzyciel zlecił czynności windykacyjne (w ramach umowy powierzenia danych). Skargi dotyczyły także nieudostępnienia danych, pomimo złożonego wniosku o ich udostępnienie.

Kolejnym zjawiskiem pojawiającym się w skargach składanych w 2019 r. było występowanie przez wierzycieli wobec spadkobierców dłużnika o ustalenie ich odpowiedzialności za długi lub w celu ustalenia kolejności dziedziczenia. Spadkobiercy zarzucali wierzycielom brak podstaw do przetwarzania ich danych osobowych. Jednakże, nawet w sytuacji odrzucenia przez nich spadku, mogli być oni przedmiotem działań prowadzonych przez wierzycieli ze względu na kwestię kolejności dziedziczenia i ustalania dalszych spadkobierców[58].

Rozstrzygnięcia wydawane przez organ w zasadniczej większości przypadków sprowadzały się do odmowy uwzględnienia wniosków skarżących ze względu na istnienie podstawy do przetwarzania danych oraz opierały się na wyjaśnieniu istoty przedawnienia roszczenia, które po jego upływie przekształca wierzytelność w zobowiązanie naturalne. W związku z czym podmioty z sektora prywatnego przetwarzały dane osobowe w celu dochodzenia roszczeń przysługujących im w stosunku do osób fizycznych praktycznie bezterminowo. Zgodnie z przepisami Kodeksu cywilnego[59] zobowiązanie naturalne nie może zostać zaspokojone 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 przy użyciu różnych środków komunikacji, co – jak można wywnioskować ze skarg rozpatrywanych przez organ w 2019 r. – było dla skarżących uciążliwe.

[58] por. decyzja Prezesa UODO z dnia 20 grudnia 2018 r. o sygn. ZSPR.440.370.2018.ME.I.
[59] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2018 r. poz. 1025).

W sprawach, w których nastąpiło przedawnienie roszczenia, zaś administrator w dalszym ciągu był uprawniony do przetwarzania danych osobowych dłużnika bez jego zgody, podstawą przetwarzania danych był prawnie usprawiedliwiony interes dochodzenia tego roszczenia, tj. wynikający z przesłanki zawartej w art. 6 ust. 1 lit. f rozporządzenia 2016/679.

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[60]. Wierzyciel ma prawo do dochodzenia swoich roszczeń również środkami pozasądowymi, zatem nie jest konieczne, by legitymował się tytułem wykonawczym w stosunku do dłużnika, chcąc dochodzić od niego roszczenia. W wielu rozstrzyganych sprawach organ oceniał także to, czy wierzyciel przetwarzając dane osobowe dłużnika wykonywał na nich operacje wyłącznie w zakresie koniecznym do dochodzenia roszczenia, w zakresie adekwatnym do tego celu[61].

Wnioski o udostępnienie danych osobowych

Jedną z istotnych kwestii rozstrzyganych przed Prezesem UODO w 2019 r. była zasadność żądania udostępnienia danych osobowych skarżącym dla zrealizowania różnego rodzaju celów[62]. Najczęściej wskazywanym celem była konieczność pozyskania danych osoby w celu wytoczenia powództwa przeciwko osobie, która naruszyła dobra osobiste wnioskującego. Zadaniem organu było ustalenie, czy administrator ustosunkował się do całego żądania strony i czy nie naruszył przepisów prawa. Przy tego rodzaju skargach konieczna była analiza okoliczności, czy zakres przedmiotowy postępowania przed organem określał żądanie skierowane uprzednio do administratora, czy może 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 postępowania nie może wywołać pożądanych skutków. 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 udostępnienia żądanych danych. Jednocześnie do wniosku skarżącego organ przychylał się wtedy, gdy

[60] por. decyzja Prezesa UODO z dnia 27 listopada 2019 r. sygn.: ZSPR.440.49.2019.ME.I.
[61] por. decyzja Prezesa UODO z dnia: 12 września 2019 r. sygn. ZSPR.440.400.2019; 4 stycznia 2019 r. sygn. ZSPR.440.631.2018; 17 stycznia 2019 r. sygn. ZSPR.440.1264.2018; 11 marca 2019 r. sygn. ZSPR.440.958.2018.
[62] por. decyzja Prezesa UODO z 21 marca 2019 r. sygn. ZSPR.440.195.2019 i decyzja Prezesa UODO z 27 sierpnia 2019 r. sygn. ZSPR.440.782.2019.

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.

Nie była zatem dla organu wystarczająca jedynie chęć wytoczenia powództwa do sądu powszechnego przeciwko osobie, której dane dotyczą[63], ponieważ na zasadność udostępnienia danych muszą wskazywać okoliczności faktyczne w sprawie. 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 oceniał także takie sytuacje, w których administratorzy – w obawie przed nieuprawnionym udostępnieniem danych osobowych – nie udostępniali ich na żądanie skarżących, pomimo spełnienia przesłanek uprawniających skarżących do żądania tych danych. Administratorzy wykazywali się zwykle daleko idącą ostrożnością w tym względzie, pozostawiając ocenę zasadności udostępnienia danych osobowych rozstrzygnięciu organu ochrony danych[64].

Przy udostępnianiu informacji o osobach korzystających z forów internetowych należy mieć także na uwadze ochronę innych praw i wolności jak np. wolność wypowiedzi. Ochrona żadnej z tych wartości nie ma charakteru bezwzględnego. Warunkami odstąpienia od bezwzględnej ochrony danych osobowych 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[65]. Odmowa udostępnienia danych osobowych może nastąpić dopiero po dokonaniu oceny zasadności żądania[66].

Banki

Najliczniej wnoszone w 2019 r. skargi dotyczyły spraw związanych z kwestionowaniem przez skarżących przetwarzania ich danych osobowych przez banki na podstawie art. 105a ust. 3 Prawa bankowego[67], a konkretnie przetwarzania danych osobowych dłużników w zbiorach danych dłużników, którzy nie wywiązali się ze zobowiązań wobec banku. Aby było możliwe przetwarzanie

[63] por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 14 kwietnia 2014 r. sygn. akt II SA/Wa 2093/13.
[64] por. decyzja Prezesa UODO z 21 marca 2019 r. sygn. ZSPR.440.195.2019; decyzje Prezesa UODO z: 11 lipca 2019 r. sygn. ZSPR.440.579.2018 oraz ZSPR.440.985.2019, decyzja Prezesa UODO z 26 czerwca 2019 r. sygn. ZSPR.440.1026.2018.
[65] por. wyrok Naczelnego Sądu Administracyjnego z dnia 22 marca 2018 r. sygn. akt I OSK 454/16.
[66] por. wyrok Naczelnego Sądu Administracyjnego z dnia 11 grudnia 2018 r. sygn. akt I OSK 398/17.
[67] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2018 r. poz. 2187 z późn. zm.), dalej jako: „Prawo bankowe".

danych osobowych osoby fizycznej na podstawie przepisu prawa bankowego, konieczne jest poinformowanie jej o zamiarze przetwarzania dotyczących jej danych osobowych bez jej 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.

Banki zazwyczaj nie dysponują dowodem doręczenia osobie, której dane dotyczą, wskazywanej informacji, przedkładając w postępowaniu przed organem wydruki z wewnętrznych systemów mających wskazywać na okoliczność skierowania do niej ww. informacji, które to dowody nie są uznawane za wystarczające z uwagi na charakter przepisów prawa bankowego. Stanowisko Prezesa UODO dotyczące konieczności możliwego do udowodnienia powiadomienia skarżących o zamiarze przetwarzania ich danych osobowych w bazach dłużników, zostało potwierdzone w wyrokach sądów administracyjnych[68]. Co istotne, odnosząc się do prowadzonych spraw można zaobserwować minimalną zmianę podejścia podmiotów sektora bankowego w zakresie 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, dysponując przy tym dowodami potwierdzającymi tę okoliczność. Nieliczne banki zaczęły informować osoby fizyczne o powyższym zamiarze przetwarzania ich danych osobowych poprzez wysyłkę korespondencji za potwierdzeniem odbioru. Jest to niewątpliwie słuszna praktyka, choć na obecną chwilę jeszcze nie powszechna. Banki nadal powołując się na art. 105a ust. 3 Prawa bankowego, wskazują na brak wyraźnego sposobu i form zawiadomienia osoby fizycznej. Należy jednak w każdym przypadku wziąć pod uwagę, że bank powinien umożliwić zweryfikowanie faktu poinformowania klienta banku o zamierzonym przetwarzaniu jego danych osobowych lub też przynajmniej przedłożyć potwierdzenie, że klientowi umożliwiono zapoznanie się z taką informacją dla celów dowodowych[69].

Innym istotnym zagadnieniem w prowadzonych postępowaniach, w których stroną był bank, były również skargi na legalność przetwarzania przez banki danych osobowych niedoszłych klientów, także w systemie informacji kredytowej (w BIK), gdy w następstwie złożenia wniosku kredytowego nie doszło do zawarcia umowy z bankiem. Banki, pomimo kierowania do nich wniosków o usunięcie danych osobowych, uznawały, że nie ma podstaw do realizacji powyższego,

[68] 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".

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

gdyż wpisy były dokonywane za zgodą klientów. Z powyższym nie zgadzał się Prezes UODO, który w wydanych decyzjach[70] nakazywał usunięcie danych osobowych niedoszłych kredytobiorców, bowiem ani banki, ani BIK, nie mają podstaw prawnych do przetwarzania powyższych danych w zakresie zapytań kredytowych oraz przetwarzania ich przez BIK po dokonaniu weryfikacji zdolności kredytowej. Stanowisko organu zostało potwierdzone w wyroku Naczelnego Sądu Administracyjnego[71], który utrzymał w mocy wyrok Wojewódzkiego Sądu Administracyjnego[72], orzekając, że gdy w następstwie złożenia wniosku kredytowego nie dochodzi do zawarcia umowy z bankiem, nie ma przesłanek ustawowych legalizujących dalsze przetwarzanie przez bank danych osobowych niedoszłego klienta.

Wśród innych skarg dotyczących sektora bankowego znaczącą część stanowiły także skargi z żądaniem zaprzestania przetwarzania danych osobowych w celach marketingowych. Dane były przetwarzane w tym celu pomimo braku zgody wyrażonej już na etapie zawierania umowy produktu bankowego lub pomimo złożonego sprzeciwu wobec przetwarzania w tym celu. Banki z reguły wyjaśniały, że takie sytuacje wynikają z błędów systemowych lub ludzkich. Znacząca liczba skarg dotyczyła także żądań klientów banków w zakresie realizacji ich prawa do usunięcia danych. W takich przypadkach Prezes UODO najczęściej odmawiał uwzględnienia żądania[73], gdyż banki wykazywały obowiązki ciążące na nich z przepisów prawa, które uzasadniają przetwarzanie przez nie danych osobowych w określonym celu i czasie (w tym przepisy o rachunkowości i o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu).

Telemarketing

W roku 2019 wpływały skargi dotyczące przetwarzania danych osobowych w celach marketingowych bez zgody osoby, której dane dotyczą. Pomimo tego, że zgodnie z Prawem telekomunikacyjnym działania telemarketingowe są dozwolone wyłącznie za uprzednią zgodą abonenta[74], a rozporządzenie 2016/679 daje osobom fizycznym uprawnienie do żądania usunięcia danych osobowych z bazy administratora, nadal występowały liczne problemy związane z realizacją powyższych uprawnień.

Naruszenia prawa w telemarketingu dotyczyły zbyt szerokich zgód na przetwarzanie danych osobowych, a także niedopełnienia obowiązków informacyjnych – w szczególności wtedy, kiedy

[70] DOLiS-440-1379/14
[71] por. wyrok Naczelnego Sądu Administracyjnego z dnia 27 sierpnia 2019 r. sygn. akt I OSK 2567/17.
[72] por. wyrok Wojewódzkiego Sądu Administracyjnego z dnia 12 lipca 2017 r. II SA/Wa 2221/16.
[73] por. decyzja Prezesa UODO z dnia 18 października 2019 r. sygn. ZSPR.440.834.2019 oraz decyzja Prezesa UODO z dnia 30 września 2019 r. sygn. ZSPR.440.114.2018.
[74] Art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954 z póź. zm.).

dane nie były pozyskane od osoby, której dotyczą, tylko z innego źródła. W takim przypadku osoba, do której dane należały, w ogóle nie miała świadomości, że zostały one pozyskane przez telemarketera. Źródłem baz danych osobowych używanych do celów telemarketingu byli tzw. brokerzy informacji, którzy pozyskiwali dane osobowe korzystając z dostępnych publicznych źródeł, ale wykorzystywali także własne sposoby pozyskiwania danych, takie jak: konkursy, ankiety, czy darmowe porady. Broker informacji, który udostępniał dla celów telemarketingu bazy z numerami telefonów, zwykle gwarantował, że zgoda była udzielona. W rzeczywistości jednak okazywało się, że albo zgoda została udzielona nieprawidłowo albo broker nie potrafił wykazać otrzymania takiej zgody od osoby, której dane dotyczą.

Poważnym problemem było również to, że administratorzy, wykorzystując bazy danych osobowych brokerów, telefonując do osób, nie podają pełnych informacji o danych kontaktowych (o nazwie, adresie, siedzibie). Działają przez podmioty przetwarzające, którym zlecają wykonywanie telemarketingu, stąd nie zawsze było można ustalić, kto jest administratorem danych odpowiedzialnym za proces przetwarzania danych osób, których dane dotyczą.

Telemarketerzy nie udzielali jednoznacznych odpowiedzi lub nie odpowiadali na pytania, które wiązały się z procesami przetwarzania danych, obowiązkami informacyjnymi lub wręcz kończyli połączenie telefoniczne po poruszeniu tych kwestii. Często też administratorzy nie odnotowywali sprzeciwu wobec przetwarzania danych osobowych w celach marketingowych, lub też nie uwzględniali żądania usunięcia danych, pomimo braku podstaw do przetwarzania danych osób, do których kierowane były połączenia telefoniczne, czy wiadomości przesyłane drogą elektroniczną (e-mail). Realizacja prawa do usunięcia danych była przez administratorów lub podmioty przetwarzające bezzasadnie utrudniana, a niekiedy administratorzy żądali kontaktowania się w tym celu z płatną infolinią.

Przykłady najczęściej udzielanych nieprawdziwych (niezgodnych ze stanowiskiem Prezesa UODO) odpowiedzi przez telemarketerów w przypadku zarzucenia im naruszenia prawa do ochrony danych osobowych brzmiały: numer telefonu nie jest daną osobową oraz, że użyty numer telefonu został wygenerowany automatycznie[75].

Istotnym zagadnieniem, które pozostaje w sferze zainteresowania organu nadzorczego było to, czy administratorzy realizują właściwie prawa osób, których dane dotyczą z punktu widzenia

[75] Co budzi jednak wątpliwości w świetle przekazu marketingowego, który często jest dopasowany swoją treścią do odbiorcy – jego miejsca zamieszkania, czy też preferencji. Może to wskazywać na dokonywanie przez podmioty przetwarzające dane, procesu zautomatyzowanego podejmowania decyzji – profilowania, o czym osoby nie są uprzednio informowane.

wyrażenia sprzeciwu do przetwarzania danych przez taką osobę. Mając na uwadze treść art. 21 ust. 4 rozporządzenia 2016/679 – administrator – najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, powinien wyraźnie poinformować ją o prawie do wyrażenia sprzeciwu, o którym mowa w art. 21 ust. 1 i 2 rozporządzenia 2016/679 (wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e lub f, w tym profilowania na podstawie tych przepisów oraz prawie do sprzeciwu na przetwarzanie danych na potrzeby marketingu bezpośredniego) przedstawić je jasno i odrębnie od wszelkich innych informacji. Zatem prawo do wyrażenia sprzeciwu na przetwarzanie danych wymaga szczególnej uwagi po stronie administratorów, powinno zmierzać do świadomego zarządzenia danymi przez administratorów, związanego z respektowaniem prawa osoby, której dane dotyczą.

Pierwszą czynnością administratora danych po otrzymaniu sprzeciwu powinno być zatem jego **odnotowanie**. Administrator danych musi być przygotowany do odnotowania sprzeciwu niezależnie od tego, jakim kanałem informacyjnym został on złożony. Natomiast pracownicy odpowiedzialni za kontakt z klientem powinni być poinformowani o możliwości złożenia takiego sprzeciwu, konieczności jego odnotowania w systemach informatycznych administratora danych oraz nadaniu mu dalszego biegu.

Prezes UODO zajął także stanowisko, że administrator nie może „zatrzymać danych" osób, które cofnęły zgodę, argumentując to tym, że potencjalnie może ponownie wykorzystać te dane. Jeśli bowiem – potencjalnie – administrator miałby po raz kolejny pozyskać i przetwarzać dane osobowe tych osób, musiałaby posiadać w stosownych okolicznościach podstawę prawną[76]. W tej sytuacji, administrator nie może argumentować pozostawienia danych osób, których dane dotyczą w bazie marketingowej, w celu uniknięcia ponownego wykorzystania tych danych, ponieważ byłoby to wbrew zasadom minimalizacji danych i zasadzie celowości ich przetwarzania.

Na tle prowadzonych w Urzędzie postępowań można było również zaobserwować sytuację, w której telemarketerzy, pomimo zgłoszonych sprzeciwów na przetwarzanie danych w celach marketingowych, nie informowali o nich administratora lub podmiotów z nimi współpracujących (np. podmioty przetwarzające) tylko nadal prowadzili wobec osób, których dane dotyczą, kampanie marketingowe. W związku z tym dochodziło do sytuacji, w których podmioty współpracujące z administratorem na podstawie zawartych umów, w dalszym ciągu przetwarzały dane osobowe dla celów marketingowych, co stanowiło rażące naruszenie przepisów rozporządzenia 2016/679. Mając na uwadze treść art. 28 ust. 3 lit e rozporządzenia 2016/679, podmiot przetwarzający, biorąc pod

[76] por. decyzja Prezesa UODO z dnia 26 lipca 2019 r. o sygn: ZSPR.440.266.2018.BN.I.

uwagę charakter przetwarzania, w miarę możliwości pomagał administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III, tj. prawa do uzyskania informacji, prawa dostępu do danych, prawa do sprostowania danych, usunięcia danych, ograniczenia przetwarzania danych, przenoszenia danych oraz prawa sprzeciwu. Wobec powyższego zasadnym jest postulat, aby podmioty te respektowały prawa osób, których dane dotyczą i w pierwszej kolejności poinformowały administratora o wyrażonym przez osobę sprzeciwie. W przeciwnym razie podejmują ryzyko, które podlegać może działaniom korygującym i kontrolnym organu. W związku z powyższym telemarketerzy czy podmioty z nimi współpracujące muszą pamiętać, że w przypadku zgłoszonego sprzeciwu nie wolno im już przetwarzać tych danych do powyższych celów.

Ubezpieczenia

Skargi rozpatrywane w roku 2019 przez Urząd w zakresie ubezpieczeń dotyczyły głównie następujących kwestii:

- niewystarczającego poziomu spełniania obowiązków informacyjnych – informacje w opinii skarżących są niejasne i zbyt ogólne, szczególnie w kwestii powierzania danych osobowych skarżących osobom nieuprawnionym,
- kwestionowania przekazywania danych osobowych skarżących pomiędzy ubezpieczycielami a podmiotami z nimi współpracującymi, szczególnie z instytucjami służby zdrowia, podmiotami uczestniczącymi w ocenie i likwidacji szkód, pośrednikami,
- pozyskiwania zbyt dużego zakresu danych osobowych, nieadekwatnego do potrzeb, często na zapas, w tym danych dotyczących zdrowia,
- przekazywania lub powierzania danych osobowych podmiotom trzecim w celach windykacyjnych,
- przetwarzania danych osobowych przez pośredników ubezpieczeniowych, którzy nieprawidłowo identyfikują osoby wnioskujące o zawarcie ubezpieczenia lub wykorzystują posiadane dane osobowe klientów towarzystw ubezpieczeniowych w celu zawierania fikcyjnych umów,
- przetwarzania danych osobowych w celu wystawiania polis ubezpieczeniowych OC komunikacyjnej, jako kontynuacji: po wygaśnięciu polisy i braku jej wypowiedzenia, oraz po zmianie własności pojazdu,

- wysyłania informacji handlowej i marketingowej bez wymaganych zgód oraz wbrew wyrażonym sprzeciwom,
- nieudzielania lub utrudniania otrzymania odpowiedzi na żądania skarżących, na podstawie ich uprawnień wynikających z rozporządzenia 2016/679,
- ujawniania danych osobowych wskutek omyłkowego wysyłania dokumentów i pism do osób trzecich,
- niedostatecznego informowania klientów o podstawach prawnych i okresie przetwarzania danych po ustaniu umowy ubezpieczenia, w szczególności danych dotyczących zdrowia.

Nie można określić, które z powyższych zagadnień dominują wśród rozpatrywanych spraw, gdyż są to na ogół pojedyncze i nieliczne przypadki. Trudno też określić wyraźną tendencję, w którą zmierzają rodzaje naruszeń prawa dotyczącego ochrony danych osobowych w sektorze ubezpieczeń. Można tylko stwierdzić, że poziom współpracy ubezpieczycieli z organem stale się poprawia. Należy jednak zaznaczyć ciągle niedostateczną znajomość przepisów rozporządzenia 2016/679. W szczególności ubezpieczyciele mają problemy z interpretacją przepisu art. 6 ust. 1 lit. c rozporządzenia i często nie podają podstawy prawnej, z której wynika obowiązek przetwarzania przez nich danych osobowych, powołując się jedynie na ten przepis.

Ze względu na rosnącą świadomość obywateli dotyczącą ochrony danych osobowych, należy się spodziewać coraz częstszego kwestionowania konieczności pozyskiwania szerokiego zakresu danych osobowych, bez wyraźnego uzasadnienia, w szczególności danych dotyczących zdrowia. Towarzystwa ubezpieczeniowe powinny także zmodyfikować swoją politykę informacyjną. Szczególnie istotne jest informowanie o podstawach prawnych i celach powierzania danych podmiotom trzecim, w celu realizacji obowiązków wynikających z prawa ubezpieczeniowego, a także o podstawach prawnych i celach przetwarzania danych po upływie okresu ubezpieczenia.

Monitoring sąsiedzki

W 2019 r. w większości przypadków skargi dotyczyły monitoringu prowadzonego przez osoby fizyczne w granicach sąsiadujących ze sobą nieruchomości. Skarżący głównie podnosili, że ich wizerunek był przetwarzany niezgodnie z prawem, ponieważ monitoring obejmował swoim zasięgiem sąsiednie nieruchomości oraz miejsca publiczne, np. drogę publiczną, chodnik, części wspólne budynków, itd. Skarżący nie wyrażali zgody na montaż monitoringu przez właścicieli sąsiednich nieruchomości, nie został wobec nich spełniony obowiązek informacyjny, nie zostało też zrealizowanie uprawnienie w postaci prawa dostępu do nagrań.

Podkreślenia wymaga fakt, że w przypadkach sporów sąsiedzkich strony postępowania z reguły pozostają w silnym konflikcie, często pomiędzy stronami toczy się kilka postępowań, w tym postępowania karne. Niekiedy zainstalowanie monitoringu na nieruchomości zostało nawet zasugerowane przez funkcjonariuszy policji biorących udział w licznych interwencjach. Osoby, które zainstalowały monitoring w składanych przed organem wyjaśnieniach wskazują, że został on zainstalowany w celach ochrony własności mienia, zdrowia i życia właścicieli nieruchomości.

W przypadku monitoringu sąsiedzkiego, który aktualnie nie posiada odrębnej regulacji w przepisach szczególnych, należy przeprowadzić postępowanie dowodowe w celu ustalenia, czy zakresem monitoringu sąsiedzkiego objęty jest wyłącznie teren prywatnej posesji, czy kamery monitoringu sąsiedzkiego obejmują również przestrzeń publiczną. Zgodnie bowiem z art. 2 ust. 2 lit. c rozporządzenia 2016/679[77], tj. w przypadku przetwarzania danych osobowych przez osoby fizyczne w ramach czynności o charakterze czysto osobistym lub domowym przepisy o ochronie danych osobowych zostają wyłączone.

Wskazać jednak należy, że zgodnie ze stanowiskiem Trybunału Sprawiedliwości UE wyrażonym w wyroku w sprawie C-212/13 Ryneš, „wykorzystywanie systemu kamer przechowującego zapis obrazu osób na sprzęcie nagrywającym w sposób ciągły, takim jak dysk twardy, zainstalowanego przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, który to system monitoruje również przestrzeń publiczną, nie stanowi przetwarzania danych w trakcie czynności o czysto osobistym lub domowym charakterze w rozumieniu tego przepisu”[78]. Tym samym, jako podstawę prawną przetwarzania danych osobowych pochodzących z monitoringu sąsiedzkiego obejmującego swoim zakresem również przestrzeń publiczną wskazać należy przesłankę legalności określoną w art. 6 ust. 1 lit. f rozporządzenia 2016/679, uznając zapewnienie bezpieczeństwa osób i mienia w obszarze objętym monitoringiem za prawnie usprawiedliwiony cel administratora danych.

Prezes UODO w dalszym ciągu prowadzi działania mające na celu wyjaśnienie powyższych kwestii zmierzających do wydania rozstrzygnięć, co do możliwości korzystania z monitoringu wizyjnego przez osoby fizyczne.

---

[77] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej jako „rozporządzenie 2016/679” lub „RODO”. (Dz.U.UE.L.2016.119.1 oraz Dz. Urz. L 127 z 23.05.2018, str. 2).

[78] Wyrok Trybunału Sprawiedliwości z dnia 11 grudnia 2014 r. w sprawie C-212/13 František Ryneš przeciwko Úřad pro ochranu osobních údajů.

Operatorzy pocztowi oraz firmy kurierskie

Do UODO wpływały również skargi dotyczące szeroko pojętych usług kurierskich i pocztowych. Obejmują one w przeważającym zakresie problematykę ujawnienia danych osobowych zawartych na przesyłkach poprzez doręczenie ich osobom nieuprawnionym (w tym pozostawienie na portierni lub u ochrony osiedla, niewyrzucenie 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 była również kwestia zabezpieczenia danych osobowych oraz ochrona danych osobowych znajdujących się w przesyłce. Należy zauważyć, że podmiot realizujący usługę nie ma wiedzy, czy i jakie dane zawiera list lub paczka.

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).

Brokerzy danych

Kolejną kategorią podmiotów, które pozostawały w zainteresowaniu Urzędu byli brokerzy danych. Za brokera danych uważany jest podmiot zajmujący się masowym zbieraniem danych osobowych oraz ich udostępnianiem (za opłatą) 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.

Do pierwszej grupy podmiotów można zaliczyć administratorów, którzy pozyskują dane osobowe z rejestrów jawnych (CEIDG), do drugiej zaś – administratorów, którzy zajmują się pozyskiwaniem danych osobowych osób fizycznych poprzez prowadzenie ankiet, konkursów, quizów, sondaży, itp.

Najczęstszy mechanizm pozyskania danych polega na tym, że po udzieleniu odpowiedzi na kilka (3-7) pytań, osoba fizyczna jest zachęcana możliwością wygrania nagrody (pieniężnej lub rzeczowej) do podania danych (imię, nazwisko, adres, telefon, e-mail, data urodzenia) oraz

zaznaczenia zgód marketingowych. Na podstawie zebranych danych administrator profiluje osoby (adres, wiek, płeć), których dane posiada i czasowo je udostępnia podmiotowi trzeciemu.

Prowadzone w Urzędzie postępowania badające legalność przetwarzania danych osobowych przez brokerów danych, ujawniły naruszenia przepisów w zakresie pozyskiwania zgód osób, których dane dotyczą oraz spełnienia obowiązków informacyjnych[79].

Prawo prasowe[80]

W 2019 r. odnotowano skargi osób fizycznych na przetwarzanie ich danych osobowych (w zakresie imienia, nazwiska, wizerunku, komentarzy) w materiałach prasowych, w tym publikowanych w serwisach internetowych.

Analiza treści wniosków skarżących i wyjaśnień administratorów (redaktorów, dziennikarzy, wydawnictw) skłaniała do konkluzji, że skarżący ograniczają możliwość przetwarzania ich danych osobowych jedynie na podstawie wyrażonej przez nich zgody, nie widząc innych podstaw prawnych wskazanych w rozporządzeniu 2016/679.

Wskazać jednak należy, że istnieje wyłączenie dotyczące realizowania prawa do bycia zapomnianym w odniesieniu do działalności dziennikarskiej, uregulowane w art. 17 ust. 3 lit. a RODO. Zgodnie z tym przepisem osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności opisanych w tym przepisie. Jednakże ustęp 1 i 2 przepisu art. 17 rozporządzenia 2016/679 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne, m.in. do korzystania z prawa do wolności wypowiedzi i informacji.

W odniesieniu do tych kwestii Prezes UODO powoływał się na wyrok z dnia 13 maja 2014 r. w sprawie C-131/12[81] oraz wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 28 czerwca 2018 r.[82]

---

[79] por. decyzja Prezesa UODO z 15 marca 2019 r. sygn. akt ZSPR.421.3.2019.

[80] Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (Dz. U. z 2018 r. poz. 1914).

[81] Jak bowiem wskazał Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 13 maja 2014 r. w sprawie C-131/12, cyt.: „*usunięcie (...) może, w zależności od rodzaju wyszukiwanej informacji, oddziaływać na uzasadniony interes potencjalnie zainteresowanych uzyskaniem dostępu do tej informacji internautów, (...) należy dążyć do znalezienia punktu równowagi pomiędzy tym interesem a prawami podstawowymi, które przysługują tej osobie na podstawie art. 7 i 8 karty. Choć niewątpliwie chronione na mocy tych postanowień prawa osoby, której dotyczą dane, są również, co do zasady nadrzędne wobec tego interesu internautów, to jednak równowaga ta może, w szczególnych przypadkach, zależeć od charakteru rozpatrywanych informacji i od tego, jak istotne są one dla prywatności osoby, której dane dotyczą, oraz dla publicznego interesu w dysponowaniu tą informacją, który to z kolei interes może być uzależniony w szczególności od roli odgrywanej przez tę osobę w życiu publicznym*".

4.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa

Zatrudnienie

Publikacja danych osobowych na stronie internetowej Biuletynu Informacji Publicznej w związku z rekrutacją pracowników korpusu służby cywilnej była przedmiotem skarg kierowanych do UODO.

Zgodnie z art. 29 ustawy o służbie cywilnej[83], wyniki naboru do ww. organów wymienionych w art. 2 ust. 1 pkt 3a ww. ustawy, oraz imiona i nazwiska kandydatów, którzy spełniają wymagania formalne, stanowią informację publiczną w zakresie objętym wymaganiami określonymi w ogłoszeniu o naborze. Zgodnie natomiast z art. 7 ust. 1 pkt 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[84], informacje publiczne podlegają publikacji w Biuletynie Informacji Publicznej. Powyższe regulacje zobowiązujące do publikacji danych dotyczących naboru nie określają okresu, w którym dane osoby biorącej udział w rekrutacji mogą być udostępniane, dlatego do określenia tego okresu zastosowanie znajdują przepisy RODO. Proces przetwarzania danych osobowych musi być zgodny z zasadami ustanowionymi w art. 5 ust. 1 RODO, dane osobowe powinny być zatem przetwarzane w jasno określonym celu, w zakresie adekwatnym dla tego celu, a także jedynie przez okres czasu niezbędny do spełnienia wyznaczonego celu. To, że określone dane odpowiadają celowi, dla którego są zbierane i są dla tego celu adekwatne, nie warunkuje, iż mogą być przetwarzane (w tym też udostępniane) innym podmiotom. Czasowym wyznacznikiem jest w takim przypadku osiągnięcie zamierzonego celu, zatem na administratorze danych ciąży obowiązek rozważenia celowości i ustanowienia okresu udostępniania danych osobowych oraz ich niezwłocznego usuwania po upływie ustanowionego okresu.

W ocenie organu właściwego do spraw ochrony danych osobowych, celem udostępnienia danych kandydatów, którzy spełnili wymagania formalne naboru, była realizacja zasady jawności, która umożliwia sprawowanie społecznej kontroli prawidłowości przebiegu postępowania rekrutacyjnego. Czas publikacji takich danych powinien być wystarczający do umożliwienia

---

[82] Z kolei wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z dnia 28 czerwca 2018 r. (M.L. i W.W. przeciwko Niemcom, połączone skargi nr 60798/10 i 65599/10) przyczynia się do wyraźnego określenia granic „prawa do bycia zapomnianym" i wskazuje, że musi ono pozostać w sprawiedliwej równowadze z innymi ważnymi interesami publicznymi, takimi jak dziennikarska wolność wyrażania opinii w demokratycznym społeczeństwie oraz prawo demokratycznego społeczeństwa do informacji na ważne tematy publiczne. Wyrok ten może stanowić zatem podstawę do skonkretyzowania (przez przyszłe judykaty) delikatnej równowagi, jaka musi zostać zachowana pomiędzy prawem jednostek do prywatności a prawem społeczeństwa do informacji (zob. Warecka Katarzyna, omówienie, opublikowano: LEX/el. 2018).

[83] Dz.U. z 2018 r. poz. 1559

[84] Dz. U. z 2018 r. poz. 1330

przeprowadzenia takiej kontroli w czasie niezbyt odległym od dokonanego wyboru, tzn. w czasie, kiedy kandydaci lub osoby trzecie mogą być zainteresowane danym naborem i będą chciały skorzystać z prawa do takiej informacji, jakie przysługuje im na podstawie art. 31 ustawy o służbie cywilnej. W ocenie Prezesa UODO optymalnym czasem, przez jaki informacje mogą być ujawniane na podstawie art. 31 ustawy, jest okres trzech miesięcy liczony od dnia ich publikacji. Na taki okres może wskazywać art. 33 ustawy o służbie cywilnej, dotyczący wyjątku od zasady obowiązku przeprowadzenia naboru. Jednocześnie pamiętać należy, że przepis art. 29 ustawy o służbie cywilnej uznaje wyniki naboru za informację publiczną, a zatem każda osoba zainteresowana wynikiem naboru może złożyć wniosek o udostępnienie takich informacji w sytuacji, kiedy zostaną one usunięte z Biuletynu urzędu, Biuletynu Kancelarii czy przestaną być dostępne w siedzibie urzędu, do którego przeprowadzany był nabór. Wobec powyższego, kontynuowanie przetwarzania danych osobowych kandydata na stronie internetowej Biuletynu Informacji Publicznej po upływie ww. okresu, Prezes Urzędu Ochrony Danych Osobowych uznawał za zbędne i niezgodne z obowiązującymi przepisami o ochronie danych osobowych i w konsekwencji nakazywał ich usunięcie[85].

W odniesieniu do sektora zatrudnienia, w 2019 r. organ właściwy do spraw ochrony danych osobowych otrzymywał również skargi dotyczące realizacji przez pracodawców żądań pracowników dotyczących prawa do uzyskania kopii danych osobowych, zawartych w prowadzonych przez pracodawców aktach osobowych. Na pracodawcy ciąży obowiązek prowadzenia i przechowywania dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników, który uregulowany został w art. 94 ust. 9a ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy[86]. W art. 94^{12} tej ustawy uregulowany został także obowiązek wydania na wniosek m.in. pracownika lub byłego pracownika, kopii całości lub części dokumentacji pracowniczej. Prezes UODO wskazywał, że realizacja powyższego prawa nie jest równoznaczna z udostępnieniem kopii danych zawartych w dokumentacji pracowniczej, zgodnie z art. 15 ust. 3 RODO. Co istotne, pracodawca będący administratorem, nie ma również na podstawie art. 15 ust. 3 RODO obowiązku udostępniania osobie zainteresowanej nośnika, na którym przetwarzane są dane osobowe oraz danych, które nie stanowią danych osobowych w rozumieniu art. 4 pkt 1 RODO i nie dotyczą wnioskującego. Realizując obowiązek wynikający z art. 15 ust. 3 RODO, administrator może poprzestać na wskazaniu treści danych dotyczących osoby, z wyłączeniem

[85] ZSZZS.440.370.2018
[86] Dz. U. z 2018 r. poz. 917

pozostałych informacji zawartych na nośniku. Administrator może jednak zrealizować ten obowiązek poprzez sporządzenie kopii lub odpisu dokumentu (nośnika) zawierającego dane osobowe. Podkreślenia wymaga, że przekazanie przez pracodawcę jedynie wykazu dokumentów zawierających dane osobowe pracownika, nie jest prawidłową praktyką i nie oznacza realizacji obowiązku wynikającego z art. 15 ust. 3 RODO, w przypadku którego podstawowe znaczenie ma treść danych[87].

Zdrowie

Zabezpieczenie danych osobowych pacjentów znajdujących się w dokumentacji medycznej było przedmiotem wielu skarg kierowanych do UODO. Dane osobowe zawarte w dokumentacji medycznej dotyczące stanu zdrowia pacjenta podlegają szczególnej ochronie prawnej. W przypadku utraty przez administratora kontroli nad nośnikami danych, istnieje wysokie prawdopodobieństwo, że informacje o stanie zdrowia zostaną udostępnione lub pozyskane przez osoby nieupoważnione. Dlatego środki służące zabezpieczeniu ww. danych przed ich utratą czy też dostępem osób nieupoważnionych, zarówno w stanie prawnym przed 25 maja 2018 r. jak i aktualnie, powinny być adekwatne do kategorii danych podlegających ochronie.

Podobnie jak w poprzednich latach sprawozdawczych, także w 2019 roku utrzymał się silny trend składania skarg na udostępnianie przez podmioty lecznicze danych osobowych dzieci oraz ich rodziców przez podmioty przeprowadzające szczepienia ochronne na rzecz organów inspekcji sanitarnej. Opiekunowie prawni małoletnich dzieci wskazywali na brak podstaw prawnych do przetwarzania danych osobowych ich dzieci w celu wykonania obowiązku szczepień. Prezes Urzędu Ochrony Danych Osobowych w wydawanych decyzjach podkreślał, że przetwarzanie danych osobowych w celu egzekwowania wykonania obowiązku szczepień znajduje oparcie w powszechnie obowiązujących przepisach. Przepisy ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, nakładają na osoby przeprowadzające szczepienia ochronne szereg związanych z tą okolicznością obowiązków, między innymi dokonywania wpisów potwierdzających wykonanie szczepienia, sporządzania sprawozdania z przeprowadzonych szczepień ochronnych oraz sporządzania sprawozdania ze stanu zaszczepienia osób objętych profilaktyczną opieką zdrowotną, które następnie osoby prowadzące szczepienia ochronne zobowiązane są przekazać państwowemu powiatowemu inspektorowi sanitarnemu[88].

[87] ZSZZS.440.842.2018

[88] Art. 17 ust. 8 ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi.

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 przywołanej wyżej ustawy, 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. Dane pozyskiwane przez państwowego powiatowego inspektora sanitarnego (lub 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, iż dane osobowe w zakresie numeru telefonu nie mogą być przez osoby przeprowadzające szczepienia ochronne udostępniane. Brak jest podstawy prawnej zezwalającej na udostępnienie przez te osoby danych osobowych w zakresie numeru telefonu i następnie ich przetwarzanie przez państwowego powiatowego inspektora sanitarnego[89].

Do Urzędu Ochrony Danych Osobowych wpłynęła też skarga dotycząca doręczania niezabezpieczonej (np. bez koperty) korespondencji zawierającej dane osobowe rodziców i dzieci, w tym informacji o niewykonaniu obowiązkowych szczepień ochronnych, w sposób umożliwiający zapoznanie się z nimi przez osoby nieuprawnione. Odnosząc się do sposobu zabezpieczania na czas wysyłki danych osobowych znajdujących się w korespondencji, Prezes UODO wskazywał, że zgodnie z art. 24 ust. 1 RODO administrator danych jest zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne, zapewniające zgodność operacji przetwarzania z obowiązującymi przepisami. Co więcej, art. 5 ust. 1 lit. f RODO nakłada na administratora danych obowiązek zapewnienia poufności i integralności danych osobowych, które są przez niego przetwarzane. Oznacza to, że administrator powinien dołożyć wszelkich starań, by zapewnić 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. Przesyłanie korespondencji zawierającej

[89] ZSZZS.440.250.2019

dane osobowe należące do katalogu danych zwykłych (imię, nazwisko, adres zamieszkania, data urodzenia), jak również danych szczególnych (informacje o niewykonanych szczepieniach ochronnych), powinno odbywać się z poszanowaniem przepisów o ochronie danych osobowych i zapewniać odpowiedni poziom zabezpieczeń. W ocenie Prezesa Urzędu Ochrony Danych Osobowych, umieszczenie wypełnionego wezwania w kopercie jest podstawowym i koniecznym elementem w celu zapewnienia poufności i bezpieczeństwa danych osobowych, w tym danych szczególnej kategorii. Prezes UODO uznał praktykę wysyłania niezabezpieczonej korespondencji za naruszającą przepisy o ochronie danych osobowych, wobec czego udzielił administratorowi upomnienia oraz skierował do niego wystąpienie w celu zapewnienia prawidłowego przetwarzania danych osobowych[90].

Szkolnictwo

W analizowanym okresie sprawozdawczym Prezes UODO rozstrzygał w sprawie dotyczącej skargi kandydata na studia, na udostępnienie przez uczelnię wyższą na stronie internetowej, po przeprowadzeniu rekrutacji, listy rankingowej kandydatów, na której znajdował się numer PESEL kandydata.

Organ nie kwestionował jawnego charakteru wyników postępowania rekrutacyjnego, gdyż kwestia ta została uregulowana pierwotnie w art. 169 ust. 16 ustawy z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym[91] i regulację tę następnie utrzymano w przepisie art. 72 ust. 5 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce[92]. Ustawodawca nie wskazał jednak dokładnej metody zrealizowania zasady jawności postępowania rekrutacyjnego, pozostawiając wybór odpowiednich środków technicznych i organizacyjnych uczelniom, których dotyczą ww. przepisy. Istotnym jest jednak, aby zrealizowanie zasady jawności postępowania rekrutacyjnego na uczelnię wyższą odbyło się z poszanowaniem dla innych przepisów, w tym przepisów o ochronie danych osobowych. Dane studentów mogą być zatem udostępnione w celu realizacji obowiązku wynikającego z przepisu prawa, jednak ich zakres, jak również sposób udostępnienia oraz czas przez jaki są upublicznione powinny być adekwatne do takiego celu. Obowiązek ten wynikał z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych z 1997 r., który nakładał na administratora obowiązek zapewnienia, aby przetwarzane dane osobowe były merytorycznie poprawne i adekwatne do celu, dla którego są przetwarzane. Obecnie

[90] ZSZZS.440.784.2018

[91] Dz. U. z 2016 r. poz. 1842

[92] Dz. U. z 2018 r. poz. 1668 z późn. zm.

taką dyspozycję reguluje art. 5 ust. 1 lit c RODO. W ocenie Prezesa UODO udostępnienie danych osobowych kandydata w zakresie numeru PESEL nie było konieczne ani niezbędne do osiągnięcia ww. celu. Jednakże zakres danych osobowych, które podlegają udostępnieniu powinien być dostosowany do określonego celu, zatem w ocenie Prezesa UODO dopuszczalnym było opublikowanie danych osób biorących udział w postępowaniu rekrutacyjnym w zakresie imienia i nazwiska[93].

W innej skardze zgłoszono nieprawidłowości w procesie przetwarzania danych osobowych rodzica ucznia, polegające na niewypełnieniu przez szkołę obowiązku informacyjnego określonego w art. 15 ust. 1 RODO, w związku z pozyskaniem danych rodzica w anonimowej ankiecie. W przedmiotowej sprawie, pomimo okoliczności, że rodzic sam umieścił swoje dane w anonimowej ankiecie, a następnie przekazał ją szkole, która po stwierdzeniu, że ankieta zawiera dane osobowe rodzica, niezwłocznie ją zniszczyła, Prezes UODO nakazał szkole spełnienie wobec ww. rodzica obowiązku informacyjnego, wynikającego z art. 15 ust. 1 RODO. Organ wskazywał, że na mocy art. 15 ust. 1 RODO 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 informacji określonych w art. 15 ust. 1 lit. a-h. Organ podnosił, że jeżeli administrator nie przetwarza danych dotyczących osoby, która zwraca się z żądaniem udzielenia informacji, to działanie administratora ograniczyć się powinno do odpowiedzi przeczącej i nie ma on obowiązku podawać podmiotowi danych innych informacji. W ocenie organu powyższy przepis nakłada na administratora, w sytuacji gdy wcześniej przetwarzał on dane wnioskodawcy, ale zaprzestał ich przetwarzania, obowiązek poinformowania o ww. okolicznościach osobę, której dane dotyczą[94].

4.1.4. Sektor organów ścigania i sądów

Rozstrzyganie skarg dotyczących kwestii ochrony danych osobowych przez formacje (służby) odpowiedzialne za bezpieczeństwo publiczne i ściganie szeroko rozumianych czynów zabronionych, odbywało się poprzez wydawanie przez Prezesa UODO decyzji administracyjnych. Pomimo że w okresie sprawozdawczym obowiązywały już przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[95], ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych

[93] ZSZZS.440.45.2019
[94] ZSZZS.440.832.2018
[95] Dz. U. z 2019 r. poz. 1781

przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[96] oraz 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 osobowych)[97], kwestie stanowiące przedmiot części skarg i kontroli, były rozpatrywane jeszcze w niektórych przypadkach na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[98]. Taki stan rzeczy wynika z brzmienia art. 175 ustawy z 10 maja 2018 r., zgodnie z którym 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 dnia 29 sierpnia 1997 r. o ochronie danych osobowych zachowały moc w odniesieniu do przetwarzania danych osobowych przez ww. organy i służby w celu wykonywania ich ustawowych zadań, do dnia wejścia w życie przepisów wdrażających dyrektywę 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 uchylającą decyzję ramową Rady 2008/977/WSiSW[99].

Implementacja przepisów wdrażających ww. dyrektywę nastąpiła dopiero 6 lutego 2019 r., tj. w dniu wejścia w życie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[100]. Z powyższego względu skargi wniesione do Prezesa UODO w 2019 r. przed 6 lutego 2019 r., dotyczące przetwarzania danych osobowych w ramach 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, były rozpatrywane na podstawie dotychczas obowiązujących przepisów.

W okresie sprawozdawczym część skarg była rozpatrywana z uwzględnieniem przepisów obowiązującego od 25 maja 2018 r. ogólnego rozporządzenia o ochronie danych osobowych. Przepisy te miały zastosowanie głównie przy rozpatrywaniu spraw dotyczących przetwarzania danych osobowych przez sądy (bez związku ze sprawowaniem przez nie wymiaru sprawiedliwości).

---

[96] Dz. U. z 2019 r. poz. 125
[97] Dz. Urz. UE L 119 z 4.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.
[98] Dz. U. z 2016 r. poz. 922 z późn. zm.
[99] Dz. Urz. UE L 119 z 04.05.2016, str. 89.
[100] Dz. U. z 2019 r. poz. 125

W okresie sprawozdawczym 2019 r. przedmiot działalności orzeczniczej Prezesa UODO, o której wyżej mowa, koncentrował się głównie na kwestiach związanych z przetwarzaniem danych osobowych przez Policję, Służbę Więzienną, sądy, prokuraturę oraz straże gminne (miejskie).

Policja

W przypadku Policji, skargi na działania poszczególnych jednostek organizacyjnych tej formacji dotyczyły najczęściej przetwarzania danych osobowych w bazach Krajowego Systemu Informacyjnego Policji (KSIP) oraz w bazach Krajowego Centrum Informacji Kryminalnych (KCIK).

Skarżący najczęściej zarzucali Policji odmowę udzielenia im informacji, czy ich dane osobowe są przetwarzane w KSIP lub w KCIK, a także brak podstaw do odmowy zaprzestania przetwarzania danych w tych systemach. Wydając decyzje w przedmiotowych sprawach, Prezes UODO brał pod uwagę przede wszystkim brzmienie art. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji[101] oraz art. 2 ust. 2 ustawy z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych[102], zgodnie z którymi dane osobowe mogą być przetwarzane zarówno w KSIP, jak i w KCIK bez wiedzy i zgody osób, których te dane dotyczą. W odniesieniu do spraw dotyczących KCIK uwzględniano również treść art. 14 ustawy o przetwarzaniu informacji kryminalnych, określającego dopuszczalny okres przetwarzania danych osobowych w KCIK, jak również treść art. 25 tej ustawy, regulującego zasady usuwania danych osobowych z baz tego systemu. Wyżej wymienione przepisy obu ustaw są przepisami szczególnymi w stosunku do postanowień ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz ustawy z 14 grudnia 2018 r. – 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. Komendant Główny Policji, jako administrator danych w przedmiocie udzielenia informacji o przetwarzaniu danych lub usunięcia danych z baz KSIP i KCIK, bierze pod uwagę przydatność 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[103]. W rozdziale 5 ww. rozporządzenia

[101] Dz. U. z 2019 r. poz. 161 z późn. zm.
[102] Dz. U. z 2019 r. poz. 44 z późn. zm.
[103] Dz. U. z 2018 r. poz. 1636

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. 211 ust. 2 i art. 21m tej ustawy.

Postępowania wszczynane w rezultacie złożonych skarg w ww. przedmiocie, kończyły się najczęściej wydaniem decyzji nieuwzględniających żądań skarżących. Działo się tak tym bardziej, że skargi w dużym stopniu były oparte o argumentację nieznajdującą podstaw w przepisach prawa. W szczególności skarżący powoływali się m.in. na art. 26 ustawy o Policji, argumentując, że w sytuacji, gdy osoba, której dane dotyczą, wystąpi z żądaniem dotyczącym realizacji przysługujących jej praw w odniesieniu do tych danych, które przetwarza Komendant Główny Policji, to z wyłączeniem okoliczności przewidzianych w ww. przepisie, brak jest podstaw do odmowy przez Komendanta Głównego Policji spełnienia żądania tej osoby. Prezes UODO odmawiając wydania decyzji nakazującej Policji poinformowanie o fakcie przetwarzania danych albo o zakresie i celu przechowywanych danych, wskazywał na art. 13 ust. 1 ustawy z 14 grudnia 2018 r., w myśl którego właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Podstawę prawną do przetwarzania danych osobowych osób, wobec których były prowadzone postępowania przez organy Policji, stanowi wspomniany już wyżej art. 20 ust. 1 ustawy o Policji, zgodnie z którym Policja, z zachowaniem ograniczeń wynikających z art. 19, może uzyskiwać informacje, w tym także niejawnie, gromadzić je, sprawdzać oraz przetwarzać. Policja może pobierać, uzyskiwać, gromadzić, przetwarzać i wykorzystywać w celu realizacji zadań ustawowych informacje, w tym dane osobowe – o osobach podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego – także bez ich wiedzy i zgody (ust. 2a). Komendant Główny Policji nie ma obowiązku udzielenia skarżącym informacji dotyczących ewentualnego przetwarzania ich danych osobowych w KSIP. Wynika to wprost z art. 20 ust. 2a ustawy o Policji. Ponadto, zgodnie z treścią art. 26 ust. 1 ustawy z 14 grudnia 2018 r., nie przekazuje się informacji, o których mowa w przepisach rozdziału 4 (prawa osoby, której dane dotyczą) oraz nie udostępnia się danych osobowych, jeżeli mogłoby to powodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;

2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6) istotne naruszenie dóbr osobistych innych osób.

Powyższy przepis reguluje ograniczenia obowiązków informacyjnych administratora danych. Biorąc pod uwagę ustawowe zadania Policji oraz fakt, iż administratorem danych przetwarzanych w KSIP jest Komendant Główny Policji, ujawnienie informacji odnośnie przetwarzanych danych w wewnętrznym systemie Policji jakim jest KSIP, w ocenie Prezesa UODO, może powodować spełnienie się przesłanek, o których mowa w powyższym przepisie. Taki stan rzeczy przemawia zatem za przychyleniem się do stanowiska Komendanta Głównego Policji, iż odmowa udzielenia informacji jest prawnie zasadna.

Skarżący wskazywali niekiedy w uzasadnieniach swoich skarg, że pozostawienie ich danych w KSIP może powodować utrudnienie bądź wręcz uniemożliwienie osiągnięcia awansu zawodowego albo zmiany rodzaju pełnionej służby w ramach różnego rodzaju umundurowanych formacji. Twierdzili także, iż dane mogą być brane pod uwagę w procesie rekrutacji oraz że stan taki jest, w ich opinii, wyrazem nierówności wobec prawa. W uzasadnieniach decyzji w ww. sprawach Prezes UODO podnosił, że informacje, które są umieszczone w KSIP, nie stanowią źródła wiedzy powszechnie dostępnej, gdyż służą wyłącznie realizacji zadań Policji, o których mowa w art. 1 ust. 2 ustawy o Policji. O ile bowiem dostęp do informacji o karalności osoby z Krajowego Rejestru Karnego ma charakter powszechny, to informacje pozyskane i wytworzone przez organy Policji w KSIP są zamkniętym, ogólnie niedostępnym zbiorem informacji i danych, służącym jedynie organom Policji dla realizacji ich ustawowych zadań związanych z zapewnieniem bezpieczeństwa i porządku publicznego.

Natomiast zupełnie innej kwestii dotyczyła skarga na nieprawidłowości w procesie przetwarzania danych osobowych przez komendanta powiatowego Policji, które polegały na pozostawieniu przez funkcjonariusza w drzwiach domu skarżącego kserokopii wezwania na badanie psychiatryczne w sposób umożliwiający zapoznanie się z jego treścią osobom nieuprawnionym. Skarżący w treści skargi dodatkowo wskazał, że ww. kserokopia nie została nawet umieszczona

w kopercie. W związku z powyższym skarżący zwrócił się do Prezesa UODO o podjęcie działań mających na celu zaniechanie takiego działania i usunięcie ich skutków oraz przestrzeganie praw skarżącego. Należy zaznaczyć, że doręczenie wezwania na badanie psychiatryczne skarżącemu za pośrednictwem jednostki organizacyjnej komendy powiatowej Policji nastąpiło na zlecenie prokuratury, w związku z toczącym się postępowaniem przygotowawczym przeciwko skarżącemu.

Prezes UODO rozstrzygając skargę wskazał, że w tym przypadku zastosowanie mają przepisy ustawy z 14 grudnia 2018 r. o ochronie danych osobowych. W art. 13 ust. 1 tej ustawy stwierdza się, że właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Należy zatem przypomnieć, że obowiązkiem Policji wynikającym z przepisu prawa, poza wykonywaniem czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz administracyjno-porządkowych, jest także, zgodnie z art. 14 ustawy z dnia 6 kwietnia 1990 r. o Policji, wykonywanie czynności pomocniczych, m.in. na polecenie sądu lub prokuratora, których zakres wynika z odrębnych ustaw. Zlecenie doręczenia korespondencji dla skarżącego przez prokuraturę znajduje oparcie w art. 131 k.p.k., jednak sposób doręczenia polegający na pozostawieniu przez funkcjonariusza Policji w drzwiach domu pisma skierowanego do skarżącego, nie miał podstawy prawnej. W konsekwencji było to działanie nieprawidłowe zarówno z świetle przepisów normujących postępowanie karne, jak i ustawy z 14 grudnia 2018 r. o ochronie danych osobowych – nie zabezpieczono bowiem danych osobowych przed ich udostępnieniem osobom nieupoważnionym. W wyniku przeprowadzonych czynności wyjaśniających Prezes UODO stwierdził naruszenie przepisów regulujących zasady ochrony danych osobowych. Jednak z uwagi na okoliczność, że doręczenie korespondencji bez wymaganej prawem formy oraz w sposób naruszający przepisy o ochronie danych osobowych miało charakter incydentalny oraz że komendant powiatowy Policji odpowiadający za działania funkcjonariusza w ww. przedmiocie podjął działania mające na celu wyeliminowanie tego typu uchybień w przyszłości, Prezes UODO uznał, że niecelowe jest wydanie decyzji nakazującej przywrócenie stanu zgodnego z prawem i odmówił uwzględnienia wniosku skarżącego w zakresie żądania skargi.

Służba Więzienna

W skargach dotyczących przetwarzania danych osobowych przez Służbę Więzienną (SW) skarżący najczęściej zarzucali naruszenie ochrony ich danych przy okazji udostępniania osadzonym informacji o stanie ich kont depozytowych. Wskazywali, że podczas pisemnego potwierdzania stanu ich depozytów pieniężnych i składania w tym celu własnoręcznych podpisów we właściwych, imiennych rubrykach stosownych list w formie papierowej, dochodziło do ujawnienia ich danych

osobowych innym osadzonym. Osadzeni dokonywali potwierdzenia stanu przynależnych im depozytów pieniężnych na ostatni dzień kwartału. Czynności te wykonywane były przy użyciu wydrukowanych wykazów sald i zajęć z programu komputerowego „Depozyt". Wykazy miały formę listy zawierającej m.in. imię, nazwisko, imię ojca oraz kwotę środków pieniężnych. Potwierdzanie przez osadzonych własnoręcznym podpisem stanu sald ich środków polegało na przedstawieniu im w obecności funkcjonariusza SW do wglądu i podpisu części listy, zawierającej dotyczące ich informacje. Natomiast znajdujące się w wykazie dane innych osadzonych były zakrywane przez funkcjonariusza np. za pomocą kartek papieru.

Rozstrzygając przedmiotowe sprawy Prezes UODO stwierdzał, że stosowanie opisanej praktyki zasłaniania na wykazach stanów kont depozytowych danych innych osadzonych, było działaniem zapewniającym – co do zasady – właściwą ochronę tych danych. Prezes UODO dopatrzył się natomiast uchybień w postaci braku zatwierdzonych procedur dotyczących zasad udostępniania osadzonym ww. wykazów zawierających dane dotyczące stanu kont. Uchybienia te niejednokrotnie były usuwane jeszcze na etapie postępowań administracyjnych i przed ich zakończeniem, przez co kończyły się one wydaniem decyzji umarzających z uwagi na niestwierdzenie na dzień ich wydania nieprawidłowości.

Sądy

Odrębną kategorię skarg rozpatrywanych przez Prezesa UODO, stanowiły skargi na przetwarzanie danych osobowych przez sądy. W większości przypadków wydawane w ich sprawie decyzje były umarzające z uwagi na fakt, iż Prezes UODO nie ma kompetencji rzeczowej do ich rozpatrywania. Zgodnie bowiem z orzecznictwem sądów administracyjnych oraz art. 175 dd § 1 ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych[104], Prezes UODO nie jest organem powołanym do rozstrzygania kwestii przetwarzania danych osobowych przez sądy w ramach sprawowanego przez nie wymiaru sprawiedliwości. Naczelny Sąd Administracyjny w wyroku z 2 marca 2001 r.[105] stwierdził, że Generalny Inspektor Ochrony Danych Osobowych (obecnie: Prezes UODO) nie jest organem kontrolującym ani nadzorującym prawidłowość stosowania prawa materialnego i procesowego w sprawach należących do właściwości innych organów, służb czy sądów, których orzeczenia podlegają ocenom w toku instancji czy w inny sposób określony odpowiednimi procedurami.

[104] Dz. U. z 2019 r. poz. 52 z późn. zm.
[105] sygn. akt II SA 401/00

Powyżej wskazane przepisy oraz ich wykładnia przesądzały o zasadności umarzania przez Prezesa UODO postępowań w sprawach skarg dotyczących sądów. Należy bowiem wskazać, że zdecydowana większość wspomnianych skarg dotyczyła właśnie czynności wykonywanych przez sądy w ramach sprawowania wymiaru sprawiedliwości, a więc np. sposobu sporządzania i treści dokumentów generowanych w toku postępowań, zasad udostępniania stronom postępowań akt spraw, zasad prowadzenia przez sądy czynności dowodowych i pozyskiwania dowodów.

Obok skarg niemogących znaleźć rozstrzygnięcia zgodnego z żądaniami skarżących, Prezes UODO w 2019 r. rozpatrywał także skargi dotyczące takich działań sądów związanych z przetwarzaniem danych osobowych, które nie mieściły się w zakresie czynności dotyczących sprawowania przez nie wymiaru sprawiedliwości, a które były jedynie czynnościami o charakterze techniczno-organizacyjnym, związanym z funkcjonowaniem sądów wyłącznie w wymiarze administracyjnym. Czynności takie, zgodnie z obowiązującymi w 2019 r. przepisami, mogły i były przedmiotem postępowań prowadzonych przez Prezesa UODO, w wyniku których zostały wydane decyzje administracyjne.

Przykładem postępowania wszczętego w wyniku skargi złożonej na sąd, dotyczącej przetwarzania danych osobowych bez związku ze sprawowaniem wymiaru sprawiedliwości, była sprawa dotycząca umieszczania numeru księgi wieczystej na kopertach z pismami wysyłanymi do uczestników postępowania sądowego. Wspomniane działanie miało zastosowanie w kilkunastu tysiącach przypadków. Według wyjaśnień prezesa sądu, umieszczenie nadruku numeru księgi wieczystej na kopertach wynikało z ustawień oprogramowania służącego do obsługi pracy wydziałów sądu. Podjęto więc działania polegające na zmianie ustawień systemu informatycznego, co wyeliminowało nadruki danych w postaci numerów ksiąg wieczystych na wysyłanych z sądu kopertach wraz z korespondencją. Prezes sądu wskazał także, że przesyłki z nadrukiem numerów ksiąg wieczystych nie były pozostawiane w skrzynkach pocztowych, a ich odbiór możliwy był po formalnym jego potwierdzeniu przez ograniczony krąg podmiotów, przez co, zdaniem prezesa sądu, można przyjąć, że ryzyko zapoznania się z nadrukiem numeru księgi wieczystej na kopercie przez osoby nieupoważnione faktycznie nie wystąpiło. Prezes sądu wskazał także na zasadę jawności ksiąg wieczystych oraz § 544 zarządzenia Ministra Sprawiedliwości z dnia 19 czerwca 2019 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej[106], jako podstawę prawną zamieszczania na kopertach znaku pisma, którym jest również numer księgi wieczystej.

[106] Dz. Urz. Ministra Sprawiedliwości z 2019 r. poz. 138.

Prezes UODO stwierdził, że w myśl art. 6 ust. 1 lit. c RODO, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z warunków wymienionych w tym przepisie, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Obowiązujące w dacie wydania niniejszej decyzji zarządzenie Ministra Sprawiedliwości z dnia 19 czerwca 2019 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej, w § 544 stanowi, że na kopertach wysyłanych pism umieszcza się w lewym górnym rogu oznaczenie nadawcy (sąd, prezes sądu, dyrektor sądu) i jego adres, a pod nim znak pisma znajdującego się w kopercie. W prawej dolnej części koperty – oznaczenie i adres odbiorcy pisma ze wskazaniem kodu pocztowego. Analogiczne rozstrzygnięcie zawarte było w § 544 zarządzenia Ministra Sprawiedliwości z dnia 12 grudnia 2003 r. w sprawie organizacji i zakresu działania sekretariatów sądowych oraz innych działów administracji sądowej[107]. W świetle wyżej wymienionych przepisów Prezes UODO uznał, że brak jest podstawy prawnej wynikającej z przepisów szczególnych, uprawniającej sąd do zamieszczania numerów ksiąg wieczystych na kopertach wysyłanych do stron postępowań wieczystoksięgowych. Tym samym zakres informacji nadrukowywany na wysyłanych kopertach był nadmierny w stosunku do celu – tj. doręczenia przesyłek listownych do ich adresatów na podstawie art. 131 ustawy z dnia z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego[108] i rozporządzenia Ministra Sprawiedliwości z dnia 12 października 2010 r. w sprawie szczegółowego trybu i sposobu doręczania pism sądowych w postępowaniu cywilnym[109]. W tej sytuacji sąd, przetwarzając dane osobowe na podstawie art. 6 ust. 1 lit. c RODO, naruszył zasadę minimalizacji danych wynikającą z art. 5 ust. 1 lit. c tego aktu prawnego, a nanoszenie numerów ksiąg wieczystych na kopertach wysyłanych do uczestników postępowań sądowych nie znajduje uzasadnienia i stanowi nadmierne, wobec celu, jakim jest prawidłowe doręczenie korespondencji, przetwarzanie danych osobowych.

Prezes UODO zwrócił także uwagę na zasadę minimalizacji danych związaną z obowiązkiem przetwarzania danych adekwatnych do celu przetwarzania, przy czym zasada ta nie oznacza ograniczenia zakresu danych jedynie do danych niezbędnych do osiągnięcia celu przetwarzania. Dopuszczalne jest bowiem przetwarzanie danych osobowych, które nie są niezbędne do osiągnięcia celu przetwarzania, ale znacznie ułatwiają jego osiągnięcie. W okolicznościach wskazanych w skardze taka sytuacja nie miała jednak miejsca.

---

[107] Dz. Urz. Ministra Sprawiedliwości z 2003 r. Nr 5 poz. 22.
[108] Dz.U. z 2018 r. poz. 1360 z późn. zm.
[109] Dz. U. z 2015 r. poz. 1222 z późn. zm.

Prokuratura

W 2019 r. do Urzędu Ochrony Danych Osobowych wpłynęła skarga na nieprawidłowości w procesie przetwarzania danych osobowych przez jedną z jednostek prokuratury. Skarga dotyczyła niewłaściwego zabezpieczenia oraz bezpodstawnego udostępnienia na rzecz osoby nieuprawnionej danych osobowych skarżącego, znajdujących się w aktach postępowania przygotowawczego. Skarżący podniósł, że jego dane osobowe w postaci adresu, numeru telefonu, numeru dowodu osobistego, numeru PESEL, a także skany jego podpisów zawarte w aktach postępowania przygotowawczego, zamazano czarnym markerem w sposób umożliwiający ich odczytanie, co wobec udostępnienia tych akt osobie nieuprawnionej umożliwiło jej zapoznanie się z treścią tych danych. W toku postępowania prowadzonego przez Prezesa UODO okazało się, że okoliczności powołane w skardze znajdują potwierdzenie w wyjaśnieniach prokuratury, która wskazała, że wspomniane protokoły przed udostępnieniem ich zostały co prawda poddane anonimizacji, niemniej jednak została ona dokonana w niewłaściwy sposób.

Prezes UODO wydał w przedmiotowej sprawie decyzję umarzającą postępowanie administracyjne. W uzasadnieniu stwierdził, że żądanie skargi nie leży w sferze jego ustawowych kompetencji. Stosownie bowiem do treści art. 3 pkt 1 ustawy z 14 grudnia 2018 r. ustawy o ochronie danych osobowych, przepisów tego aktu prawnego nie stosuje się do ochrony danych osobowych zawartych w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych, prowadzonych na podstawie m.in. ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[110]. Znaczy to, iż do danych osobowych zawartych w wymienionych wyżej zbiorach danych, przetwarzanych w toku m.in. postępowania karnego, przedmiotowa ustawa nie ma zastosowania. Dane te chronione są na podstawie przepisów normujących dane postępowanie. Kwestia udostępniania akt postępowania karnego stanowi szczególny wymiar operacji na danych, przez którą należy rozumieć dostęp do danych osobowych zawartych w aktach sprawy poprzez możliwość przeglądania materiału dowodowego, uzyskiwania odpisów i kopii dokumentów zgromadzonych w aktach postępowania. Jednak wobec regulacji art. 3 pkt 1 przywołanej powyżej ustawy z 14 grudnia 2018 r. o ochronie danych osobowych, Prezes UODO nie może ingerować w czynności udostępniania dokumentów zgromadzonych w aktach postępowań, które zostały uregulowane m.in. w przepisach ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego. Zatem nawet, gdyby wątpliwość budził sposób anonimizacji dokumentów zawierających dane osobowe skarżącego oraz udostępnienie akt

[110] Dz. U. z 2018 r. poz. 1987 z późn. zm.

postępowania, to Prezes UODO nie ma kompetencji do podejmowania czynności dotyczących postępowań prowadzonych przez inne organy na podstawie aktów prawnych wskazanych w treści art. 3 pkt 1 ustawy z 14 grudnia 2018 r.

Straż miejska

W analizowanym 2019 r. orzecznictwo Prezesa UODO obejmowało również działania straży miejskich (gminnych). Z uwagi na fakt, że są to formacje powołane ustawowo do sprawowania pieczy nad bezpieczeństwem publicznym, przetwarzanie przez nie danych osobowych jest regulowane w znacznym stopniu przez przepisy ustawy z 14 grudnia 2018 r. o ochronie danych osobowych. Zgodnie z art. 10 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych[111], straż miejska wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego.

Do UODO wpłynęła m.in. skarga na przetwarzanie danych osobowych w postaci adresu zamieszkania przez straż miejską w postępowaniu w sprawie wykroczenia drogowego. Skarżący zarzucił, że straż miejska pozyskała jego dane osobowe w postaci adresu zamieszkania oraz kierowała na ten adres korespondencję w związku z popełnionymi wykroczeniami przez pracowników spółki, w której skarżący pełnił funkcję członka zarządu. Skarżący podniósł, że jego adres zamieszkania nie figuruje w Krajowym Rejestrze Sądowym i został pozyskany nielegalnie. W jego ocenie straż miejska nie miała podstaw do kierowania korespondencji w sprawie dotyczącej spółki na jego adres zamieszkania, ponieważ nie jest on ujawniony w publicznie dostępnych źródłach.

Komendant straży miejskiej, ustosunkowując się do treści skargi wskazał, że podstawą przetwarzania danych osobowych skarżącego pozyskanych ze zbioru „Powszechny Elektroniczny System Ewidencji Ludności" jest art. 44h ust. 1 pkt 2 ustawy z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych[112], zaś podstawą prawną przetwarzania danych osobowych pozyskanych ze zbioru: „Centralna Ewidencja Pojazdów i Kierowców" jest art. 80c ust. 1 pkt 10a oraz 100c ust. 1 pkt 8a ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym[113]. Wskazał także, iż w toku czynności wyjaśniających w związku z ujawnieniem wykroczenia polegającego na nieprawidłowym parkowaniu pojazdu stwierdzono, że użytkownikiem (posiadaczem) pojazdu jest spółka, w której skarżący pełni funkcję członka zarządu. Komendant podkreślił, że straż miejska

[111] Dz. U. z 2018 r. poz. 928 z późn. zm.
[112] Dz. U. z 2006 r. poz.139, poz. 993 z późn. zm.
[113] Tekst jednolity: Dz. U. z 2020 r. poz. 110.

zwróciła się pisemnie na adres spółki o wskazanie osoby, której w czasie, w jakim stwierdzono wykroczenie drogowe, powierzono do kierowania lub używania ww. pojazd, jednak wezwania pozostały bez odpowiedzi. W konsekwencji straż miejska zwróciła się bezpośrednio na adres zamieszkania skarżącego, jako członka organu reprezentującego spółkę, do której należy pojazd, celem złożenia stosownych wyjaśnień.

Kluczowe znaczenie dla rozstrzygnięcia przedmiotowej sprawy miał przepis art. 78 ust. 4 ustawy z dnia 20 czerwca 1997 r. prawo o ruchu drogowym, zgodnie z którym właściciel lub posiadacz pojazdu jest obowiązany wskazać na żądanie uprawnionego organu, komu powierzył pojazd do kierowania lub używania w oznaczonym czasie, chyba że pojazd został użyty wbrew jego woli i wiedzy przez nieznaną osobę, czemu nie mógł zapobiec. W myśl ust. 5, gdy właścicielem lub posiadaczem pojazdu jest osoba prawna – do udzielenia informacji w ww. zakresie obowiązana jest osoba wyznaczona przez organ uprawniony do reprezentowania tego podmiotu na zewnątrz, a w przypadku niewyznaczenia takiej osoby – osoby wchodzące w skład tego organu zgodnie z żądaniem organu, o którym mowa w ust. 4 oraz sposobem reprezentacji podmiotu. W świetle powyższych przepisów straż miejska była uprawniona do pozyskania danych o użytkowniku pojazdu w związku z postępowaniem wykroczeniowym. Wskazuje na to również art. 10 pkt 1 ustawy o strażach gminnych, w myśl którego straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. Zgodnie z art. 10a ust. 1 tej ustawy, straż miejska w celu realizacji ustawowych zadań może przetwarzać dane osobowe bez wiedzy i zgody osoby, której dane dotyczą, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, o ile dane te są uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia lub pochodzą z rejestrów, ewidencji i zbiorów, do których straż posiada dostęp na podstawie odrębnych przepisów.

Spółka jako posiadacz pojazdów, których kierujący nimi naruszyli przepisy prawa o ruchu drogowym, miała prawny obowiązek udzielić informacji na temat danych pracowników kierujących pojazdami w okresach, w których doszło do potencjalnych wykroczeń. Z obowiązkiem tym skorelowane było uprawnienie straży miejskiej do skutecznego żądania danych indywidualizujących sprawców tych wykroczeń. Z materiału dowodowego zebranego w sprawie wynika, że mimo starań straży miejskiej spółka – jako odbiorca wezwań – nie podjęła żadnych kroków celem zadośćuczynienia żądaniom ww. organu. W tej sytuacji straż miejska zwróciła się bezpośrednio do skarżącego jako członka zarządu spółki, z wezwaniem do udzielenia niezbędnych

informacji celem dalszego prowadzenia postępowania w sprawie wykroczeń. Podstawą przetwarzania danych skarżącego, jak i ich żądania, są przepisy art. 44h ust. 1 pkt 2 ustawy z 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych oraz art. 78 ust. 5 prawa o ruchu drogowym. W świetle powyższego pozyskanie przez straż miejską danych osobowych skarżącego w postaci adresu zamieszkania miało podstawę prawną. Celem pozyskania i przetwarzania tych danych było ustalenie sprawców wykroczeń drogowych w postępowaniach prowadzonych przez straż miejską. Zatem przetwarzanie przedmiotowych danych nastąpiło z uwagi na dobro publiczne, którym jest utrzymanie porządku publicznego oraz egzekwowanie przepisów powszechnie obowiązującego prawa. W rezultacie powyższych ustaleń Prezes UODO uznał, że nie doszło do naruszenia przepisów o ochronie danych osobowych, co czyniło postępowanie bezprzedmiotowym w całości. Z tego względu Prezes UODO umorzył postępowanie.

4.2. Zawiadomienie o podejrzeniu popełnienia przestępstwa

W analizowanym 2019 r. Prezes Urzędu Ochrony Danych Osobowych skierował do organów powołanych do ścigania przestępstw **5 zawiadomień o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych.**

Dwa z tych zawiadomień dotyczyły spraw związanych z nieuprawnionym przetwarzaniem danych osobowych przez administratora strony internetowej[114].

W jednym z tych zawiadomień[115] Prezes UODO dodatkowo wskazał na **brak określenia podmiotu administrującego i odpowiedzialnego za przetwarzanie danych osobowych klientów**, którzy korzystali z usług platformy internetowej służącej do automatycznego formułowania pozwów. Wygenerowanie pozwu za pomocą portalu wymagało wpłacenia kwoty co najmniej 59 złotych za pośrednictwem płatności elektronicznej. Błędy fleksyjne widoczne na stronie internetowej dodatkowo pozwalały przypuszczać, że twórcą platformy był program komputerowy, lub że stworzono ją przy wykorzystaniu translatora internetowego, na co wskazywała treść Polityki Prywatności zawierająca błędy składniowe. Ponadto kod strony internetowej zawierał słowa pisane cyrylicą np. „привязка к сген.эл.", co świadczyło, że autor strony nie jest narodowości polskiej. W niniejszej sprawie nie było możliwości ustalenia podmiotu administrującego stroną internetową ani stwierdzenia, czy posiada on uprawnienia do przetwarzania

[114] ZSPR.070.8.2019 i ZSPR.070.6.2019.
[115] ZSPR.070.6.2019.MD

danych osobowych, jaki jest zakres tych danych oraz czy ich przetwarzanie jest dopuszczalne w świetle obowiązujących przepisów.

Wskazać należy, iż obowiązki usługodawcy świadczącego usługi drogą elektroniczną zostały szczegółowo określone w art. 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[116] stanowiącego, iż usługodawca podaje w sposób wyraźny, jednoznaczny i bezpośrednio dostępny poprzez system teleinformatyczny, którym posługuje się usługobiorca, informacje podstawowe: 1) adresy elektroniczne; 2) imię, nazwisko, miejsce zamieszkania i adres albo nazwę lub firmę oraz siedzibę i adres. Jeżeli usługodawcą jest przedsiębiorca, podaje również informacje dotyczące właściwego zezwolenia i nazwę organu zezwalającego, w razie gdy świadczenie usługi wymaga, na podstawie odrębnych przepisów, takiego zezwolenia oraz wskazania danych identyfikacyjnych i adresowych. Jednocześnie niezrealizowanie tych obowiązków na podstawie art. 23 ustawy, stanowi czyn zabroniony zagrożony karą grzywny. Konieczne było również zbadanie działalności podmiotu prowadzącego stronę internetową, także pod względem popełnionego czynu karalnego, polegającego na niewypełnieniu obowiązków informacyjnych, jakie spoczywają na usługodawcy na gruncie przepisów ustawy o świadczeniu usług drogą elektroniczną.

W ocenie organu istniało wysoce prawdopodobne zagrożenie dla ochrony danych osób, których dane zostały pozyskane i przetwarzane w związku z funkcjonowaniem tej platformy. Podkreślenia wymaga, że Prezes UODO ma ograniczone możliwości działania w zakresie badania okoliczności i legalności przetwarzania danych osobowych, natomiast organy ścigania dysponują szerszymi możliwościami w tym zakresie. W tym stanie faktycznym i prawnym Prezes Urzędu Ochrony Danych Osobowych zdecydował o złożeniu zawiadomienia o popełnieniu przestępstwa.

Drugie z kolei **zawiadomienie**[117] **o podejrzeniu przestępstwa polegało na nieuprawnionym przetwarzaniu danych osobowych oraz handlu tymi danymi za pośrednictwem strony internetowej**. W sprawie tej ustalenie osoby oferującej sprzedaż baz danych osobowych okazało się również niemożliwe. Tak samo jak ustalenie źródła ich pochodzenia. Dlatego Prezes UODO złożył do prokuratury zawiadomienie o popełnieniu przestępstwa.

W 2019 r. Prezes UODO zawiadomiła Prokuratora Generalnego **o podejrzeniu popełnienia przestępstwa przez spółkę, która jako administrator kilkunastu stron internetowych żądała**

[116] Dz. U. z 2019 r. poz. 123
[117] ZSPR.070.8.2019.MD

pieniędzy za usunięcie wpisów zawierających dane osobowe[118]. Prawo dostępu do danych, ich sprostowania, przeniesienia czy usunięcia to niektóre z praw przysługujących obywatelom na gruncie ogólnego rozporządzenia o ochronie danych. Za korzystanie z tych praw administratorzy nie mogą żądać opłat od osób, których dane przetwarzają. Mimo to jedna ze spółek, która działała na terenie Polski, domagała się 200 zł za usunięcie wpisu na swoich portalach (ma ich kilkanaście), w których znajdowały się dane osobowe lekarzy, prawników, przedsiębiorców czy fachowców świadczących różnego rodzaju usługi. W ocenie Prezes Urzędu Ochrony Danych Osobowych spółka naruszyła nie tylko przepisy RODO, ale również Kodeksu karnego, ponieważ wprowadziła w błąd osoby, informując je o konieczności uiszczenia opłaty. A to, zdaniem Prezesa UODO, prowadzi do podjęcia przez pokrzywdzonych niekorzystnej decyzji rozporządzającej w odniesieniu do ich mienia, co jest działaniem na niekorzyść tych osób. W ocenie Prezesa Urzędu takie działanie należało uznać za wypełniające znamiona czynu z art. 286 Kodeksu karnego, czyli oszustwa.

Spółka działała w tzw. państwie trzecim (poza Europejskim Obszarem Gospodarczym), ale kierowała swoje usługi do polskich obywateli i tym samym podlegała pod regulacje RODO. Co więcej, spółka ta mogła być powiązana z podmiotami zarejestrowanymi w Polsce. Jednak Prezes UODO w ramach swoich kompetencji nie był w stanie wykazać tego powiązania, co uniemożliwiło mu podejmowanie skutecznych działań w celu obrony praw osób, których dane dotyczą. Organy ścigania mają w tym względzie znacznie większe możliwości prawne, by zweryfikować okoliczności sprawy. W związku z tym Prezes UODO przekazał Prokuratorowi Generalnemu, wraz z zawiadomieniem o podejrzeniu popełnienia przestępstwa, listę stron internetowych, którymi administruje spółka oraz wszystkie inne ustalenia organu ds. ochrony danych osobowych.

Na podstawie art. 108 ust. 1 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.[119] Prezes UODO – działając w innej sprawie – powiadomił prokuraturę o **podejrzeniu popełnienia przestępstwa polegającego na udaremnieniu przez jeden z podmiotów przeprowadzenia czynności kontrolnych przez UODO**[120]. Prokuratura podjęła czynności w tej sprawie i przesłała do sądu akt oskarżenia przeciwko osobie oskarżonej o popełnienie tego przestępstwa.

Wskazać należy, że poprzez uniemożliwienie przeprowadzenia kontroli ten sam podmiot naruszył również art. 31 w związku z art. 58 ust. 1 lit. e oraz lit. f RODO[121]. Zgodnie bowiem z art. 31 ogólnego rozporządzenia o ochronie danych, administrator i podmiot przetwarzający oraz – gdy

[118] ZSPR.070.2.2019
[119] Dz. U. z 2019 r. poz. 1781
[120] ZSPR.421.19.2019/49512/MN
[121] Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.

ma to zastosowanie – ich przedstawiciele, na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań. Obowiązek współpracy polega m.in. na zapewnieniu organowi nadzorczemu możliwości uzyskania od administratora (i podmiotu przetwarzającego) dostępu do wszystkich danych osobowych oraz wszelkich informacji niezbędnych organowi nadzorczemu do realizacji jego zadań[122], uzyskania dostępu do wszelkich 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[123]. W związku z tym Prezes UODO wszczął z urzędu postępowanie administracyjne celem nałożenia na ten podmiot administracyjnej kary pieniężnej.

Prezes UODO w roku 2019 skierował na podstawie art. 304 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego[124] **zawiadomienie o podejrzeniu popełnienia przestępstwa określonego w art. 276 Kodeksu karnego, polegającego na niwelowaniu (niszczeniu, uszkadzaniu, czynieniu bezużytecznym, ukrywaniu lub usuwaniu) dokumentu, którym sprawca tego czynu nie ma prawa wyłącznie rozporządzać.**

Powyższe zawiadomienie skierowane zostało przez organ właściwy do spraw ochrony danych wskutek powzięcia informacji o porzuceniu dokumentacji pochodzącej z jednej ze spółek, w tym m.in. dokumentacji pracowniczej, teczek osobowych, kserokopii dowodów osobistych oraz umów czy zezwoleń na pracę, faktur i innych dokumentów, obejmujących dane osobowe. Spółka, której dotyczyło zgłoszenie została rozwiązana bez przeprowadzenia postępowania likwidacyjnego i następnie wykreślona z rejestru przedsiębiorców Krajowego Rejestru Sądowego. W ocenie Prezesa Urzędu Ochrony Danych Osobowych powyższa okoliczność nie zwalniała jednak spółki i członków jej organów, zaś po rozwiązaniu spółki także jej byłych wspólników, z odpowiedzialności za należyte zabezpieczenie i przechowywanie wytworzonych lub zgromadzonych w okresie istnienia spółki dokumentów. W świetle obecnie obowiązujących przepisów, osoby te nie były ponadto uprawnione do wyrzucania, niszczenia czy też ukrywania tych dokumentów. Na podstawie przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[125] oraz Rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji

[122] art. 58 ust. 1 lit. e ogólnego rozporządzenia o ochronie danych.
[123] art. 58 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych.
[124] Dz. U. z 2018 r. poz. 1987 z późn. zm.
[125] Dz. U. z 2019 r. poz. 553 z późn. zm.

niearchiwalnej[126], znajdujące się wśród dokumentów teczki z aktami osobowymi oraz faktury zaliczyć należy do dokumentacji niearchiwalnej. Zgodnie z załącznikiem nr 1 do powołanego wyżej rozporządzenia, dokumentacją niearchiwalną jest dokumentacja o czasowym znaczeniu praktycznym, którą należy zakwalifikować do kategorii archiwalnej oznaczanej symbolem „B". Jednym z podstawowych obowiązków pracodawcy, zgodnie z poprzednio obowiązującym brzmieniem art. 94 pkt 9b Kodeksu pracy, był obowiązek przechowywania dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników w warunkach niegrożących uszkodzeniem lub zniszczeniem. Także przepisy ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych[127], regulują obowiązek przechowywania przez płatnika składek listy płac, kart wynagrodzeń albo innych dowodów, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty, przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika, z zastrzeżeniem wyjątków od tej zasady, uregulowanych w ust. 4a ww. ustawy, które przewidują w określonych przypadkach skrócenie ww. okresu do 10 lat.

Wobec okoliczności, iż przepisy ustawy o narodowym zasobie archiwalnym i archiwach nie zawierają regulacji dotyczących przekazania do dalszego przechowywania dokumentacji osobowej i płacowej na czas, jaki pozostał do końca okresu jej przechowywania ustalony na podstawie odrębnych przepisów, w przypadku rozwiązania spółki bez przeprowadzania postępowania likwidacyjnego przyjąć należy, że analogiczne zastosowanie znajdzie w takim przypadku przepis art. 51 u tej ustawy, zgodnie z którym w przypadku postawienia pracodawcy w stan likwidacji lub ogłoszenia jego upadłości, odpowiednio likwidator lub syndyk wskazuje podmiot prowadzący działalność w dziedzinie przechowywania dokumentacji, któremu zostanie ona przekazana do dalszego przechowywania, zapewniając na ten cel środki finansowe na czas, jaki pozostał do końca okresu przechowywania dokumentacji ustalonego na podstawie odrębnych przepisów. W ocenie Prezesa UODO, przed wykreśleniem spółki z rejestru, jej zarząd powinien wypełnić wymienione wyżej wskazania celem zapewnienia byłym pracownikom dostępu do ww. dokumentacji. Wskazać należy także, że zgodnie z art. 51 z ust. 1 ustawy o narodowym zasobie archiwalnym i archiwach, Naczelny Dyrektor Archiwów Państwowych może wydać decyzję nakazującą złożenie dokumentacji, która należała do pracodawcy wykreślonego z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, na odpłatne przechowywanie we

[126] Dz. U. z 2019 r. poz. 264 z późn. zm.
[127] Dz. U. z 2017 r. poz. 1383, 1386 i 2120 oraz z 2018 r. poz. 138.

wskazanym archiwum państwowym, jeżeli istnieje zagrożenie jej zniszczenia, w szczególności na skutek oddziaływania czynników atmosferycznych lub bezprawnego działania osób trzecich. W świetle przywołanego przepisu brak jest podstaw prawnych do jej przekazania innemu podmiotowi celem dalszego przechowywania. Wydanie ww. decyzji wiąże się z powstaniem obowiązku pokrycia kosztów przejęcia, zewidencjonowania, przechowania i konserwacji dokumentacji przez archiwa państwowe, które to koszty ponoszą solidarnie osoby zarządzające lub pełniące funkcje organu zarządzającego pracodawcy w dniu jego wykreślenia z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej[128].

Także przepisy ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług[129], nakładają na przedsiębiorcę obowiązki dotyczące przechowywania m.in. faktur, w sposób zapewniający łatwe ich odszukanie oraz autentyczność pochodzenia, integralność treści i czytelność od momentu ich wystawienia lub otrzymania do czasu upływu terminu przedawnienia zobowiązania podatkowego.

Zgodnie natomiast z art. 70 ust. 1 ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa[130], zobowiązanie podatkowe przedawnia się z upływem 5 lat, licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku. Jak stanowi art. 32 § 1a Ordynacji podatkowej, w razie likwidacji lub rozwiązania osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej, podmiot dokonujący likwidacji lub rozwiązania zawiadamia pisemnie właściwy organ podatkowy, nie później niż w ostatnim dniu istnienia osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej, o miejscu przechowywania dokumentów związanych z poborem lub inkasem podatku.

W świetle powyższego istniało uzasadnione podejrzenie popełnienia przestępstwa określonego w art. 276 Kodeksu karnego, zgodnie z którym kto niszczy, uszkadza, czyni bezużytecznym, ukrywa lub usuwa dokument, którym nie ma prawa wyłącznie rozporządzać, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

5. Kontrola przestrzegania przepisów 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

[128] art. 51z ust. 5 ust. 51 ustawy o narodowym zasobie archiwalnym.
[129] Dz.U z 2018 r. poz. 2174 z późn. zm.
[130] Dz.U. z 2019 r. poz. 900 z późn. zm.

zostały odrębnie uregulowane w rozdziale 9 ustawy z 10 maja 2018 r. o ochronie danych osobowych. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa UODO planem kontroli lub na podstawie uzyskanych przez niego informacji lub w ramach monitorowania przestrzegania stosowania przepisów RODO. Aktualne przepisy wzmacniają kompetencje kontrolerów UODO.

Od 1 stycznia do 31 grudnia 2019 r. przeprowadzono łącznie **98 kontroli** przestrzegania przez administratorów oraz podmioty przetwarzające, obowiązujących przepisów prawa ochrony danych osobowych – zarówno RODO, jak i przepisów sektorowych. **W podmiotach sektora prywatnego przeprowadzono 20 kontroli, sektora publicznego – 25, organów ścigania i sądów – 23, sektora zatrudnienia, zdrowia i szkolnictwa – 22 oraz 8 kontroli sprawdzających wykonanie obowiązku wynikającego z decyzji Prezesa UODO przeprowadzonych przez jednostkę egzekucyjną Urzędu.**

Dla porównania, w 2018 r. przeprowadzono łącznie 72 kontrole – 40 kontroli w okresie 1 stycznia – 24 maja 2018 r. i 32 kontrole w okresie od 25 maja – 31 grudnia 2018 r.

Kontrole prowadzone były w ramach zatwierdzonego przez Prezesa UODO planu kontroli (kontrole sektorowe), bądź na podstawie uzyskanych informacji dotyczących nieprawidłowości w procesie przetwarzania danych osobowych (kontrole doraźne). Kontrole doraźne zainicjowane są m.in. skargami bądź sygnałami od obywateli, a także przesłanymi przez administratorów zgłoszeniami naruszeń ochrony danych osobowych czy doniesieniami medialnymi.

Kontrolami przeprowadzonymi w 2019 roku objęto podmioty prowadzące telemarketing, portal internetowy, organizatora loterii, banki w zakresie profilowania klientów i potencjalnych klientów, centrum medyczne podmiotu leczniczego w ramach badania procesu wystawiania i obsługi elektronicznych zwolnień lekarskich (e-ZLA), placówki oświatowe i służby zdrowia wykorzystujące monitoring wizyjny, podmioty lecznicze w zakresie źródeł pozyskiwania i sposobu zbierania danych osobowych, spółdzielnie mieszkaniowe, urzędy miast, starostwa, urząd marszałkowski, przedsiębiorstwo wodociągów i kanalizacji, przedsiębiorstwo zarządzające kompleksowym systemem gospodarki odpadami komunalnymi, ZUS, Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych oraz Krajową Izbę Rozliczeniową.

Przeprowadzono też kontrole dotyczące przetwarzania danych osobowych przez organy administracji państwowej oraz powołane ustawą służby w zakresie, w jakim wykonują one zadania polegające na rozpoznawaniu, zapobieganiu, wykrywaniu i zwalczaniu czynów zabronionych, prowadzeniu postępowań w sprawach dotyczących tych czynów oraz wykonywaniu orzeczeń

w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania tych służb.

Większość działań kontrolnych koncentrowało się na badaniu sposobów, w jaki administratorzy danych osobowych zapewniają zachowanie poufności danych oraz czy nie wykorzystują danych w innych celach, niż te, dla których zostały zebrane. Zakres przeprowadzonych kontroli obejmował m.in. podstawę prawną przetwarzania danych osobowych; źródło pozyskania danych osobowych; zakres, cel i rodzaj przetwarzanych danych osobowych; sposób dopełnienia obowiązków administratora danych wynikających z art. 13 i art. 14 ogólnego rozporządzenia o ochronie danych; sposób zapewnienia realizacji praw osób, których dane dotyczą, określonych w ogólnym rozporządzeniu o ochronie danych; sposób zbierania i udostępniania danych osobowych; czy zostały wdrożone odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z ogólnym rozporządzeniem o ochronie danych oraz z uwzględnieniem charakteru, zakresu, kontekstu, celów przetwarzania i ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te są w razie potrzeby poddawane przeglądom i uaktualniane (art. 32 i art. 24 ogólnego rozporządzenia o ochronie danych); czy zostały wdrożone polityki ochrony danych, o których mowa w art. 24 ust. 2 ogólnego rozporządzenia o ochronie danych; czy wyznaczony został inspektor ochrony danych osobowych (art. 37 ogólnego rozporządzenia o ochronie danych); czy administrator danych powierza przetwarzanie danych podmiotom przetwarzającym, a jeśli tak, to czy powierzenie to nastąpiło przy spełnieniu warunków określonych w art. 28 ogólnego rozporządzenia o ochronie danych; czy podjęte zostały działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora, która ma dostęp do danych osobowych, przetwarzała je na polecenie administratora (art. 29 i art. 32 ust. 4 ogólnego rozporządzenia o ochronie danych); czy została przeprowadzona ocena skutków dla ochrony danych w związku z wprowadzeniem systemu zdalnego odczytu wodomierzy (art. 35 ogólnego rozporządzenia o ochronie danych); czy dokumentowane są wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (art. 33 ust. 5 ogólnego rozporządzenia o ochronie danych); czy prowadzony jest rejestr czynności przetwarzania danych osobowych, w którym zamieszczone są wszystkie informacje określone w art. 30 ust. 1 ogólnego rozporządzenia o ochronie danych; kontrola systemów informatycznych wykorzystywanych do przetwarzania danych osobowych.

Poniżej omówione zostały wybrane przykłady kontroli przeprowadzonych w podmiotach sektora publicznego, prywatnego oraz odpowiedzialnych za bezpieczeństwo publiczne i ściganie sprawców czynów zabronionych.

5.1. Sektor publiczny

Kontrole przeprowadzone w podmiotach **sektora publicznego** dotyczyły m.in. miejskiego monitoringu wizyjnego (kontynuacja kontroli sektorowych z 2018 r.), udostępniania danych w Biuletynie Informacji Publicznej oraz sposobu wysyłania korespondencji zawierającej dane osobowe, sposobu prowadzenia rejestru czynności przetwarzania danych osobowych i sposobu dokumentowania przez administratora naruszeń ochrony danych osobowych, systemu identyfikacji i monitoringu odpadów, sposobu prowadzenia i zabezpieczenia przez spółdzielnie mieszkaniowe rejestru członków oraz systemu zdalnego odczytu stanu wodomierzy.

Na skutek przeprowadzonych kontroli wszczętych zostało 10 postępowań administracyjnych, w których wydanych zostało 8 decyzji, w tym 4 decyzje umarzające postępowanie oraz 4 decyzje nakładające administracyjną karę pieniężną. W jednym z przypadków na decyzję Prezesa UODO została wniesiona skarga do Wojewódzkiego Sądu Administracyjnego. Ponadto w jednym z przypadków nie zostało wszczęte postępowanie administracyjne. Natomiast w odniesieniu do pozostałych 14 podmiotów, u których przeprowadzono czynności kontrolne, w czasie opracowania niniejszego Sprawozdania, wciąż jeszcze analizowany był materiał dowodowy zebrany podczas kontroli.

Nieprawidłowości stwierdzone w toku prowadzonych przez Prezesa Urzędu Ochrony Danych Osobowych kontroli w podmiotach sektora publicznego, dotyczyły przede wszystkim niewłaściwego dopełniania wobec osób, których dane dotyczą, **obowiązku informacyjnego**, o którym mowa w art. 13 ogólnego rozporządzenia o ochronie danych. Kontrole niejednokrotnie wykazywały, że obowiązek ten albo nie był w ogóle realizowany, albo był wykonywany w sposób nieprawidłowy ze względu na niepodawanie wszystkich wymaganych informacji wskazanych w powołanym przepisie. Kontrolowane podmioty nie podawały m.in. pełnej informacji o podstawie prawnej przetwarzania danych, informacji o odbiorcach danych osobowych oraz o okresie, przez który dane osobowe będą przechowywane czy też o skutkach niepodania danych osobowych, o ile osoba, której dane dotyczą jest zobowiązana do ich podania. W przypadku miejskiego monitoringu wizyjnego zdarzały się przypadki, w których administratorzy nieprawidłowo wskazywali, jakie prawa przysługują osobom, których dane dotyczą. Odnotowano też sytuacje, w których obowiązek

informacyjny nie był spełniany albo brak było klauzuli informacyjnej przy wszystkich punktach kamerowych[131].

Do dość częstych uchybień stwierdzonych w toku kontroli należały również nieprawidłowości związane z **rejestrem czynności przetwarzania**. Administratorzy nie ujmowali w nim wszystkich informacji wymaganych przepisami ogólnego rozporządzenia o ochronie danych, m.in. o odbiorcach danych, a ponadto błędnie określali okres retencji przetwarzanych danych osobowych. Nieprowadzenie rejestru czynności przetwarzania zgodnie z art. 30 ust. 1 RODO uniemożliwiało organowi nadzorczemu monitorowanie operacji przetwarzania[132].

Kontrolowani administratorzy nie zawierali **umów powierzenia przetwarzania** danych osobowych z podmiotami, którym przekazywane były dane osobowe np. w zakresie asysty technicznej i serwisu programistycznego strony BIP. Zdarzały się także przypadki, kiedy kontrolowany administrator, co prawda zawarł umowę powierzenia przetwarzania danych, jednak naruszył przepisy o ochronie danych poprzez nieujęcie w niej: zasad współpracy pomiędzy administratorem a podmiotem przetwarzającym w zakresie realizacji praw osób, których dane osobowe są przetwarzane; zasad wsparcia administratora w wywiązywaniu się z obowiązków określonych w art. 32–36 ogólnego rozporządzenia o ochronie danych oraz w zakresie udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwiających administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji i przyczyniania się do nich[133].

Prowadzone przez Prezesa UODO kontrole dowodzą, że administratorzy wciąż mają problemy z właściwym przeprowadzeniem **analizy ryzyka i oceny skutków**. W ocenie skutków m.in. nie zostały opisane działania naprawcze, a także nie dokonano oceny ryzyka dla poszczególnych zagrożeń czy procesów przetwarzania, jak np. przetwarzania danych w ramach miejskiego monitoringu wizyjnego czy też korzystania z portalu YouTube podczas przetwarzania danych osobowych uczestników obrad rady powiatu. Skutkiem nieprzeprowadzenia analizy ryzyka było przede wszystkim niewdrożenie przez administratora adekwatnych środków organizacyjnych i technicznych zapewniających przetwarzanie danych osobowych zgodnie z art. 24 ust. 1 i art. 32 ust. 1 RODO. Ponadto przy opracowywaniu analizy ryzyka administratorom zdarzało się powoływać na nieobowiązujące już przepisy prawa, tj. ustawę z dnia 29 sierpnia 1997 r. o ochronie

[131] np. ZSPU.421.1.2019, ZSPU.421.2.2019.
[132] np. ZSPU.421.8.2019 ZSPU.421.9.2019.
[133] np. ZSPU.421.6.2019, ZSPU.421.7.2019.

danych osobowych, natomiast nie wskazywano przepisów ogólnego rozporządzenia o ochronie danych. Wskazane uchybienia wpływały zatem na kompletność i przejrzystość analizy ryzyka[134].

Niezależnie od wszczętych postępowań administracyjnych, na podstawie dokonanych w toku kontroli ustaleń, do podmiotów kontrolowanych kierowane były zalecenia zawierające wytyczne w zakresie przyjęcia przez podmioty kontrolowane określonej praktyki działania mającej wpływ na poprawność przetwarzania danych osobowych. Zalecenia te dotyczyły m.in. konieczności dokonania pomiędzy Prezydentem Miasta a Komendantem Straży Miejskiej wspólnych uzgodnień w zakresie przetwarzania danych osobowych w ramach **miejskiego monitoringu wizyjnego** oraz konieczności dokonania każdorazowo przez administratora danych osobowych oceny, jak planowane modyfikacje systemu informatycznego, w którym przetwarzane są dane osobowe, będą wpływały na bezpieczeństwo przetwarzanych danych osobowych[135]. Warto zwrócić uwagę na fakt, iż zalecenia dotyczące wspólnych uzgodnień pomiędzy Prezydentem Miasta a Komendantem Straży Miejskiej w zakresie przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego, przedstawiane były także w toku kontroli przeprowadzonych w roku poprzednim, co może świadczyć o braku świadomości administratorów danych w tym zakresie i rodzi potrzebę przeprowadzenia kampanii informacyjnej skierowanej do podmiotów przetwarzających dane w ramach miejskiego monitoringu wizyjnego. Jednostki kontrolowane nie wywiązywały się z obowiązków określonych w przepisach o ochronie danych osobowych najczęściej z powodu błędnej ich interpretacji lub braku środków finansowych niezbędnych do pokrycia kosztów związanych z wdrożeniem rozwiązań zapewniających prawidłowe spełnienie wymogów wynikających z przepisów ogólnego rozporządzenia o ochronie danych.

Analizując wyniki przeprowadzonych kontroli, należy stwierdzić, że nadal zdarzają się administratorzy mający problemy z prawidłowym wykonaniem podstawowych obowiązków określonych w przepisach o ochronie danych osobowych, w tym z zastosowaniem odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych osobowych. Brak procedur określających sposób postępowania z danymi osobowymi, w tym ich udostępniania w związku z realizacją np. obowiązków wynikających z przepisów ustawy o dostępie do informacji publicznej, a także możliwość łatwego przełamania przez atakującego istniejących (niewystarczających) zabezpieczeń, prowadzą do udostępnienia danych osobom nieuprawnionym. Czynnikiem, który zwiększa ryzyko naruszenia przepisów o ochronie danych osobowych w danej organizacji jest także

[134] np. ZSPU.421.2.2019, ZSPU.421.8.2019.
[135] np. ZSPU.421.4.2019, ZSPU.421.2.2019.

brak świadomości osób dopuszczonych do przetwarzania danych osobowych w zakresie bezpieczeństwa ich przetwarzania, spowodowany brakiem wystarczającej liczby szkoleń pracowników w powyższym zakresie.

Podkreślenia wymaga, że cztery postępowania wszczęte w wyniku przeprowadzonych kontroli zakończyły się nałożeniem administracyjnej kary pieniężnej[136].

5.2. Sektor prywatny

W okresie od rozpoczęcia stosowania przepisów RODO, tj. od dnia 25 maja 2018 r. do 31 grudnia 2019 r. w podmiotach **sektora prywatnego** przeprowadzono 31 kontroli, z czego w samym 2019 kontrole odbyły się w 20 podmiotach (10 kontroli sektorowych i 10 kontroli doraźnych).W 2 podmiotach zaplanowane czynności kontrolne nie odbyły się, gdyż podmioty te udaremniły ich przeprowadzenie. W przypadku 4 podmiotów w wyniku przeprowadzonych kontroli nie stwierdzono naruszenia przepisów o ochronie danych osobowych. W 14 sprawach postępowanie było w toku, przy czym w przypadku dwóch podmiotów wydane zostały decyzje, na które złożono skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Telemarketing

Działania kontrolne w tym sektorze skoncentrowały się na ustaleniu źródła pozyskania danych osobowych (numerów telefonów), pod które wykonywane były połączenia w celu przedstawienia oferty marketingowej.

Skontrolowane podmioty w dużej mierze prowadziły telemarketing na rzecz innych podmiotów. Niektóre z nich do wykonywania połączeń telefonicznych wykorzystywały systemy informatyczne dostarczone przez inne podmioty, niektóre nie posiadły żadnej bazy danych (z numerami telefonów), a połączenia telefoniczne (według ich oceny) generowane były automatycznie przez system informatyczny pozyskany od innego podmiotu. Analiza umowy na użytkowanie przykładowego systemu informatycznego wykazała, że podmiot kontrolowany nie posiadał dostępu do wybieranego numeru telefonu. W umowie zawarty był zapis, z którego wynikało, że dostawca sytemu będzie administrował danymi zgodnie z obowiązującymi przepisami, a w przypadku jakichkolwiek roszczeń osób trzecich kierowanych wobec podmiotu kontrolowanego, zobowiązuje się do pokrycia wszelkich kosztów związanych z takimi roszczeniami. Prezes Urzędu Ochrony Danych Osobowych uznał za konieczne przeprowadzenie

[136] ZSPU.421.3.2019, ZSPU.421.13.2019, ZSPU.421.14.2019, ZSPU.421.16.2019; więcej zob. Cz. II, rozdz. 9 niniejszego *Sprawozdania z działalności Prezesa UODO w roku 2019,* pt. „Administracyjne kary pieniężne".

kontrolni u dostawcy tego systemu. Do kontroli jednak nie doszło, gdyż dostawca systemu udaremnił przeprowadzenie czynności kontrolnych. W związku z tym Prezes UODO podjął działania przewidziane przepisami prawa tj. zawiadomił prokuraturę o podejrzeniu popełnienia przestępstwa (naruszenie art. 108 ustawy o ochronie danych osobowych) oraz wszczął postępowanie administracyjne w zakresie naruszenia zasad współpracy z organem (art. 31 rozporządzenia 2016/679), zmierzające do nałożenia kary pieniężnej.

Przetwarzanie danych z monitoringu wizyjnego

Jedna z przeprowadzonych kontroli dotyczyła podmiotu, który zgłosił naruszenie w zakresie udostępnienia nagrań z monitoringu osobom nieupoważnionym. Naruszenie to dotyczyło upublicznienia nagrania z zakupów dokonanych na terenie jednej z placówek handlowych. W toku kontroli ustalono, że pracownik firmy ochroniarskiej aparatem telefonicznym nagrał film z obrazu zamieszczonego na ekranie monitora wchodzącego w skład systemu monitoringu stosowanego w tej placówce. Następnie nagranie to udostępnił pracownikowi tej placówki handlowej, który z kolei najprawdopodobniej przekazał przedmiotowe nagranie dziennikarzowi. W ten sposób nagranie zostało upublicznione w mediach społecznościowych. Z ustaleń kontroli wynika, że podmiot prowadzący przedmiotową placówkę handlową zawiadomił prokuraturę o podejrzeniu popełnienia przestępstwa z art. 107 § 1 ustawy o ochronie danych osobowych przez osoby, o których mowa powyżej. Wskazać należy, że w toku tej samej kontroli został przeprowadzony test w celu zbadania, czy obraz kamery zamontowanej nad kasą pozwala na odczytanie danych zamieszczonych na dokumencie zbliżonym do oka kamery. W wyniku tego testu stwierdzono, że odczyt obrazu z kamery jest bardzo nieczytelny i nie pozwala na odczytanie jakichkolwiek informacji, w tym danych osobowych zawartych w dokumencie poddanym oględzinom.

Podobnie jak w poprzednich latach, również w 2019 r. kontynuowano kontrole przetwarzania danych osobowych uzyskanych za pośrednictwem środków technicznych umożliwiających rejestrację obrazu (monitoring wizyjny) w placówkach oświatowych. W toku tych kontroli weryfikacji poddano między innymi 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 danych dokumentują wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (art. 33 ust. 5 RODO).

W opisywanym okresie sprawozdawczym prowadzono także kontrole, zakresem których objęto przetwarzanie przez pracodawców danych osobowych pracowników rejestrowanych za pośrednictwem monitoringu. W kontrolach tych badano m.in. podstawę prawną i cel przetwarzania danych osobowych oraz ich zakres i rodzaj. Ponadto weryfikacji poddany został okres przetwarzania, a także sposób udostępniania danych osobowych. Organ weryfikował także sposób dopełnienia obowiązków administratora danych wynikających z art. 12, art. 13 ust. 1 i ust. 2 oraz art. 15 ust. 2 i ust. 3 RODO. Kontroli poddawano także systemy informatyczne wykorzystywane do przetwarzania danych osobowych uzyskanych za pośrednictwem środków technicznych umożliwiających rejestrację obrazu (monitoring).

Nieuprawniony dostęp do danych

Inna kontrola przeprowadzona w związku ze zgłoszonym naruszeniem polegała na uzyskaniu przez uczestnika loterii nieuprawnionego dostępu do danych osobowych innych uczestników. Ustalono, że administrator nie w pełni wdrożył odpowiednie środki techniczne, aby zapewnić odpowiedni stopień bezpieczeństwa przetwarzanych danych, w skutek czego nastąpił incydent, który umożliwił osobie nieupoważnionej pobranie informacji zawierających dane osobowe uczestników loterii. Podmiot usunął przedmiotowe naruszenie oraz poinformował o naruszeniu osoby, których dane dotyczyły.

5.3. Sektor organów ścigania i sądów

W 2019 r. **w podmiotach odpowiedzialnych za bezpieczeństwo publiczne i ściganie sprawców czynów zabronionych, przeprowadzono łącznie 23 kontrole oraz zwrócono się do inspektora ochrony danych w jednym z podmiotów o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania.** Kontrole przeprowadzone zostały w następujących podmiotach: Policja (6 kontroli), Straż Graniczna (4 kontrole), Służba Więzienna (6 kontroli), Straż Miejska (2 kontrole) oraz wydziały (referaty) konsularne przy ambasadach Rzeczypospolitej Polskiej oraz w Ministerstwie Spraw Zagranicznych (5 kontroli).

Policja

Kontrolami przeprowadzonymi w powiatowych i miejskich komendach Policji objęto zbadanie sposobu zastosowania środków technicznych i organizacyjnych mających na celu zapobieżenie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych, a także realizację obowiązków związanych z wewnętrzną obsługą oraz zgłaszaniem Prezesowi Urzędu Ochrony Danych Osobowych naruszeń ochrony danych osobowych.

W pięciu kontrolowanych jednostkach stwierdzono brak polityki ochrony danych osobowych wydawanej na podstawie ustawy z 14 grudnia 2018 r. o ochronie danych osobowych, przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[137]. Ustalono również, że w kontrolowanych jednostkach Policji po wejściu w życie przywołanej wyżej ustawy, nowo zatrudniani pracownicy byli dopuszczani do przetwarzania danych osobowych bez nadania im stosownych upoważnień, o których mowa w art. 41 ust. 1 tej ustawy, a ponadto w większości kontrolowanych jednostek stwierdzono naruszenie art. 39 ust. 2, poprzez niewdrożenie odpowiednich środków organizacyjnych i technicznych mających na celu zabezpieczenie danych zapisywanych na elektronicznych nośnikach danych przed ich nieuprawnionym odczytaniem, kopiowaniem, zmienianiem lub usuwaniem (nośniki zewnętrzne tj. pendrive oraz dyski twarde komputerów przenośnych nie były szyfrowane). W tracie kontroli stwierdzono również dwa przypadki powierzenia przetwarzania danych osobowych bez zawarcia umowy powierzenia, o której mowa w art. 34 ust. 1 ustawy z 14 grudnia 2018 r. o ochronie danych osobowych.

Część stwierdzonych uchybień została usunięta po zakończeniu kontroli, niemniej wobec wszystkich kontrolowanych jednostek Policji Prezes Urzędu Ochrony Danych Osobowych wszczął postępowania administracyjne w zakresie stwierdzonych uchybień.

Straż Graniczna

Dwie kontrole w jednostkach Straży Granicznej, tj. w Komendzie Głównej Straży Granicznej oraz w jednej z placówek Straży Granicznej, zostały przeprowadzone w zakresie przetwarzania danych osobowych w związku z realizacją uprawnień kontrolowanych jednostek, wynikających z przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[138], tj. przetwarzaniem danych osobowych w ramach Wizowego Systemu Informacyjnego (VIS).

Kontrole koncentrowały się przede wszystkim na sprawdzeniu środków organizacyjnych i technicznych mających zapewnić zgodność z prawem danych VIS, ich dokładność i aktualność. Weryfikowano także okres przechowywania danych VIS oraz sposoby realizacji obowiązku ich usuwania po upływie okresu, na który dane te zostały wprowadzone do VIS przez kontrolowane jednostki. Zakresem kontroli objęto również środki kontroli dostępu do danych VIS oraz sposoby weryfikacji, czy wykorzystanie danych przetwarzanych w VIS jest zgodne z prawem, tzn. dostęp do danych mają tylko osoby uprawnione i osoby te wykorzystują ten dostęp w uzasadnionym celu

[137] Dz. U. z 2019 r. poz. 125
[138] Dz. U. z 2018 r. poz. 134 z późn. zm.

(w związku z prowadzoną sprawą). Nie stwierdzono nieprawidłowości w zakresie objętym kontrolami.

Dodatkowo w jednym z oddziałów Straży Granicznej oraz w jednej z placówek Straży Granicznej przeprowadzono kontrole, których zakres obejmował przede wszystkim ustalenie sposobów zastosowania środków mających na celu zapobieganie nieuprawnionemu wprowadzaniu, oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania) oraz ich zabezpieczenie podczas przekazywania lub podczas przenoszenia nośników danych (kontrola transportu). Nie stwierdzono nieprawidłowości w zakresie objętym kontrolami.

Służba Więzienna

Kontrolami objęto m.in. badanie sposobu zastosowania środków mających na celu ochronę praw i wolności osób pozbawionych wolności oraz osób ubiegających się o wstęp na teren jednostki organizacyjnej Służby Więziennej. Kontrolami w powyższym zakresie objęto dwa zakłady karne oraz jeden areszt śledczy. Stwierdzone nieprawidłowości polegały głównie na nieuwzględnieniu w polityce ochrony danych osobowych sposobów dokumentowania wszystkich środków sprawdzanych podczas kontroli. W dwóch z ww. przypadków nieprawidłowości zostały usunięte bezpośrednio po wszczęciu postępowania administracyjnego. W jednym przypadku wydana została decyzja nakazująca usunięcie uchybień.

W Centralnym Zarządzie Służby Więziennej przeprowadzona została kontrola, której zakresem objęto przetwarzanie przez Dyrektora Generalnego Służby Więziennej danych osobowych osób pozbawionych wolności wprowadzonych do Centralnej Bazy Danych Osób Pozbawionych Wolności. W trakcie kontroli stwierdzono m.in. naruszenia polegające na niezastosowaniu mechanizmów weryfikacji przydatności informacji w Centralnej Bazie oraz niepowierzenie podległym jednostkom organizacyjnym przetwarzania danych osobowych w Centralnej Bazie. Stwierdzone w trakcie kontroli uchybienia oraz inne nieprawidłowości zostały usunięte po zakończeniu czynności kontrolnych.

Przeprowadzono również kontrole w areszcie śledczym oraz w instytucji gospodarki budżetowej realizującej zadania publiczne, polegające na prowadzeniu oddziaływań penitencjarnych oraz resocjalizacyjnych. Zakresem powyższych kontroli objęto przetwarzanie danych osobowych osób pozbawionych wolności oraz danych osobowych osób zamawiających paczki dla osób pozbawionych wolności, w związku z realizacją uprawnień osób pozbawionych

wolności, określonych w art. 113a ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy[139], tj. prawa osadzonych do dokonywania zakupów oraz otrzymywania paczek.

Ustalono, że kontrolowana instytucja gospodarki budżetowej nie dostosowała swojej działalności do wymogów określonych w ustawie o ochronie danych osobowych. W trakcie kontroli ustalono m.in., że nie opracowano i nie wdrożono polityki ochrony danych osobowych, nie był prowadzony wykaz kategorii czynności przetwarzania. W kontrolowanym areszcie śledczym ustalono, że upoważnienia do przetwarzania danych osobowych nie odnoszą się do kategorii czynności przetwarzania. Ustalono również, że dyrektor aresztu, jako podmiot przetwarzający, nie uzyskał zgody administratora na dalsze powierzenie przetwarzania danych osobowych innym podmiotom.

Systemy SIS/VIS

Kontrolami objęto podmioty uprawnione do dostępu do systemów SIS/VIS. Kontrole przeprowadzone zostały w wydziałach (referatach) konsularnych przy ambasadach Rzeczypospolitej Polskiej oraz w Ministerstwie Spraw Zagranicznych. Zakresem kontroli objęto przetwarzanie danych osobowych w związku z realizacją uprawnień wskazanych podmiotów wynikających z przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[140], tj. wglądu w dane SIS i dane VIS oraz dokonywaniu wpisów danych SIS i danych VIS. Kontrole koncentrowały się przede wszystkim na sprawdzeniu czy dostęp do funkcjonalności systemu informatycznego, umożliwiającego dostęp do danych SIS i danych VIS, miały wyłącznie osoby posiadające odpowiednie uprawnienia. Sprawdzeniu poddano również sposób zastosowania środków mających na celu zapewnienie zgodności wykorzystywania danych z obowiązującymi przepisami. Ustalono, że dostęp do danych SIS/VIS posiadają wyłącznie konsulowie, a więc osoby uprawnione w świetle przepisów ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Konsulowie posiadali odpowiednie upoważnienia określone w przepisach ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym.

W wyniku kontroli przeprowadzonej w Ministerstwie Spraw Zagranicznych ustalono, że w ramach tegoż ministerstwa nie są podejmowane działania mające na celu zapewnienie zgodności

[139] Dz. U. z 2019 r. poz. 676 z późn. zm.
[140] Dz. U. z 2018, poz. 134

wykorzystywania danych z obowiązującymi przepisami przez pracowników zatrudnionych w Ministerstwie Spraw Zagranicznych. W związku ze stwierdzonym uchybieniem Prezes Urzędu Ochrony Danych Osobowych zwrócił się do Ministra Spraw Zagranicznych celem złożenia wyjaśnień.

Straż Miejska

Zakresem kontroli objęto zabezpieczanie przez komendanta straży miejskiej danych osobowych przetwarzanych w bloczkach mandatowych, w związku ze zgłoszonymi Prezesowi Urzędu Ochrony Danych Osobowych naruszeniami ochrony danych osobowych. Stwierdzono uchybienie polegające na zgłaszaniu organowi nadzorczemu naruszeń ochrony danych osobowych jedynie w przypadkach, w których w ocenie kontrolowanego podmiotu, nie wystąpiło wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą. Zgodnie z art. 44 ust. 1 z dnia 14 grudnia 2018 r. zgłaszania naruszeń organowi nadzorczemu nie dokonuje się jedynie wtedy, gdy nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych. Oznacza to, że podmiot kontrolowany zobowiązany był do dokonywania zgłoszeń również w przypadkach, gdy w wyniku zdarzenia wystąpiło nie tylko wysokie, ale jakiekolwiek ryzyko naruszenia praw i wolności osób, których dane dotyczą.

W związku z pismem Prokuratury przeprowadzono również kontrolę, której zakresem objęto udostępnienie przez komendanta straży miejskiej danych osobowych dyrektorowi zarządu transportu zbiorowego. Nie stwierdzono uchybień w procesie przetwarzania danych osobowych w zakresie objętym kontrolą.

6. Egzekucja administracyjna – zapewnienie wykonania decyzji

Prezes 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, jest wierzycielem i organem egzekucyjnym w odniesieniu do egzekucji obowiązków o charakterze niepieniężnym z zakresu ochrony danych osobowych. Dzięki temu Prezes UODO może prowadzić czynności mające na celu zapewnienia wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych[141]. Prezes UODO występuje

[141] Zadania związane z zapewnieniem wykonywania przez zobowiązanych obowiązków wynikających z decyzji administracyjnych Prezesa UODO do dnia 30 listopada 2019 r. należały do Zespołu ds. Kar i Egzekucji. Od dnia 1 grudnia 2019 r., po reorganizacji Urzędu, zadania te przypadły Departamentowi Kar i Egzekucji. Zob. Cz. I, rozdz. 2, niniejszego *Sprawozdania z działalności Prezesa UODO w roku 2019",* pt. „Urząd Ochrony Danych Osobowych".

również w roli wierzyciela i organu egzekucyjnego w odniesieniu do obowiązków o charakterze niepieniężnym nałożonych ostatecznymi decyzjami GIODO wydanymi przed dniem 25 maja 2018 r.[142] Ponadto Prezes UODO jest wierzycielem w 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 zaznaczyć, że w celu zapewnienia wykonania obowiązków wynikających z decyzji administracyjnych, Prezes UODO – poza możliwością stosowania egzekucji administracyjnej – na podstawie art. 83 ust. 6 RODO posiada 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 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

W omawianym okresie sprawozdawczym 2019 roku, egzekucji administracyjnej podlegały wszystkie decyzje administracyjne Prezesa Urzędu Ochrony Danych Osobowych – a także decyzje wydane jeszcze przez Generalnego Inspektora Ochrony Danych Osobowych przed 25 maja 2018 r. – nakładające na strony obowiązek (nakaz) do wykonania, które były ostateczne oraz te, którym nadano rygor natychmiastowej wykonalności. Jeżeli decyzja administracyjna zawierała postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlegał egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek do wykonania nakładany na stronę (zobowiązanego) może polegać w szczególności na: usunięciu uchybień w procesie przetwarzania danych osobowych, spełnieniu żądania osoby, której dane dotyczą (odnoszącego się do jej praw wynikających z przepisów o ochronie danych osobowych), wprowadzeniu czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania danych, zawieszeniu przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej, czy wreszcie – na zawiadomieniu osoby, której dane dotyczą o naruszeniu ochrony jej danych osobowych.

Prezes UODO wykonuje zadania m.in. w zakresie: wymierzania grzywien i prowadzenia postępowań z tym związanych na podstawie art. 69 ustawy o ochronie danych osobowych

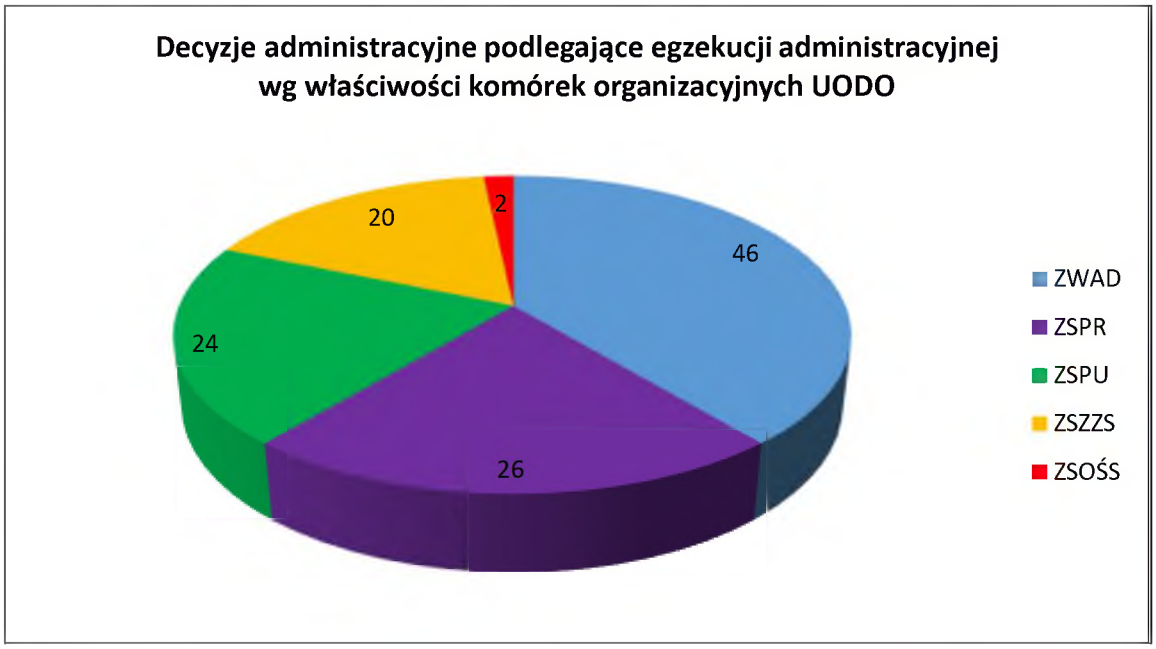
[142] Na podstawie art. 167 ust. 1 ustawy o ochronie danych osobowych, Biuro Generalnego Inspektora Ochrony Danych Osobowych stało się Urzędem Ochrony Danych Osobowych (UODO).

w związku z art. 88 k.p.a., odraczania uiszczania kar pieniężnych i rozkładania ich na raty, a także udzielania ulg w wykonaniu kar. Dodatkowym zadaniem wykonywanym w 2019 r. w komórce egzekucyjnej było rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych. W ramach tego zadania w 2019 r. prowadzonych było **99 postępowań**, z których **52 zostały zakończone**, w tym 42 wydaniem decyzji administracyjnej.

Komórka egzekucyjna UODO wykonująca zadania organu w zakresie egzekucji administracyjnej, przeprowadziła **8 kontroli** sprawdzających zgodność przetwarzania danych z przepisami o ochronie danych osobowych, z czego 7 dotyczyło sprawdzenia wykonania nakazów decyzji, w pięciu przypadkach kontrole potwierdziły wykonanie, bądź doprowadziły bezpośrednio do wykonania obowiązku wynikającego z decyzji.

W 2019 roku prowadzona była **egzekucja administracyjna 118 decyzji administracyjnych** zawierających nałożony na strony nakaz (obowiązek) do wykonania o charakterze niepieniężnym, z czego 107 postępowań dotyczyło egzekucji nakazów decyzji wydanych przez Prezesa Urzędu Ochrony Danych Osobowych, a 11 decyzji wydanych jeszcze przez Generalnego Inspektora Ochrony Danych Osobowych przed 25 maja 2018 r. Wobec 2 zobowiązanych wystawione zostały upomnienia. Postępowania, w których wystawiono upomnienie zostały zakończone w 2019 r. w związku z wykonaniem nakazów decyzji przez zobowiązanych, nie było zatem konieczności wystawiania tytułów wykonawczych.

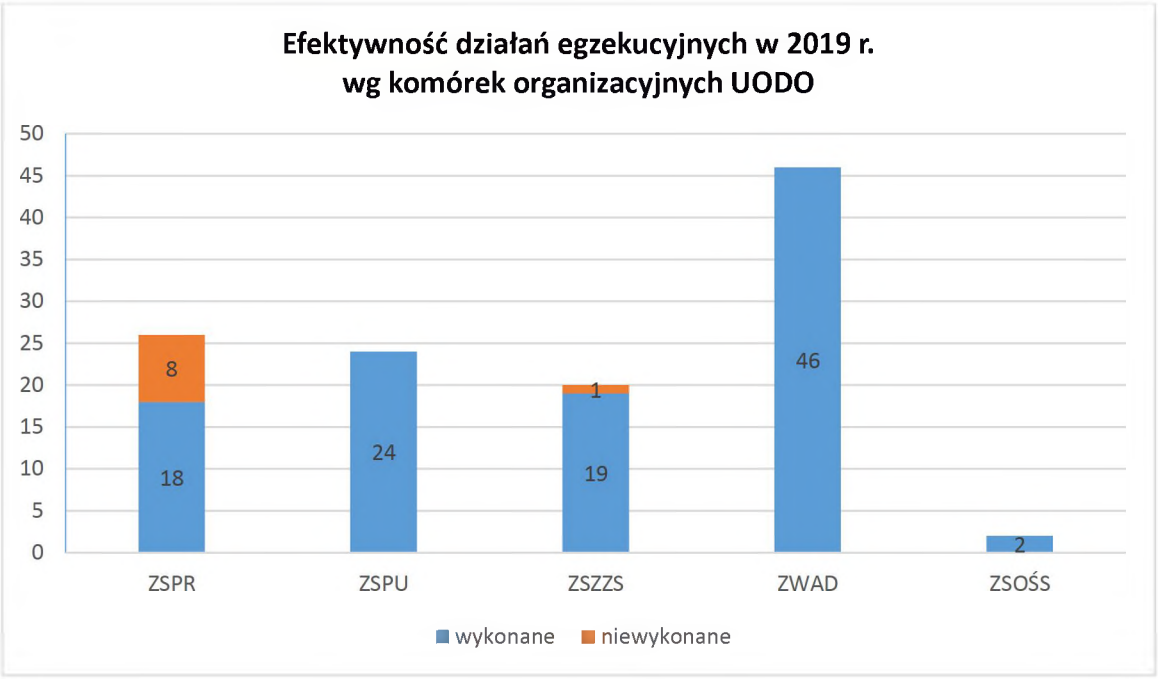
Dokonując podziału tych decyzji wg właściwości komórek UODO, to: 46 z nich dotyczyło właściwości Zespołu Współpracy z Administratorami Danych (ZWAD), 26 – Zespołu ds. Sektora Prywatnego (ZSPR), 24 – Zespołu ds. Sektora Publicznego (ZSPU), 20 – Zespołu ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa (ZSZZS) oraz 2 – Zespołu ds. Sektora Organów Ścigania i Sądów (ZSOŚS). Nowością w stosunku do roku 2018 było przekazanie do egzekucji decyzji wydanych przez Zespół Współpracy z Administratorami Danych oraz Zespołu ds. Sektora Organów Ścigania i Sądów. Wszystkie decyzje przekazane do egzekucji przez Zespół Współpracy z Administratorami Danych dotyczyły naruszeń ochrony danych osobowych zgłaszanych przez administratorów, a największa liczba takich decyzji wskazuje na dużą świadomość wśród administratorów istnienia obowiązku zgłaszania naruszeń.



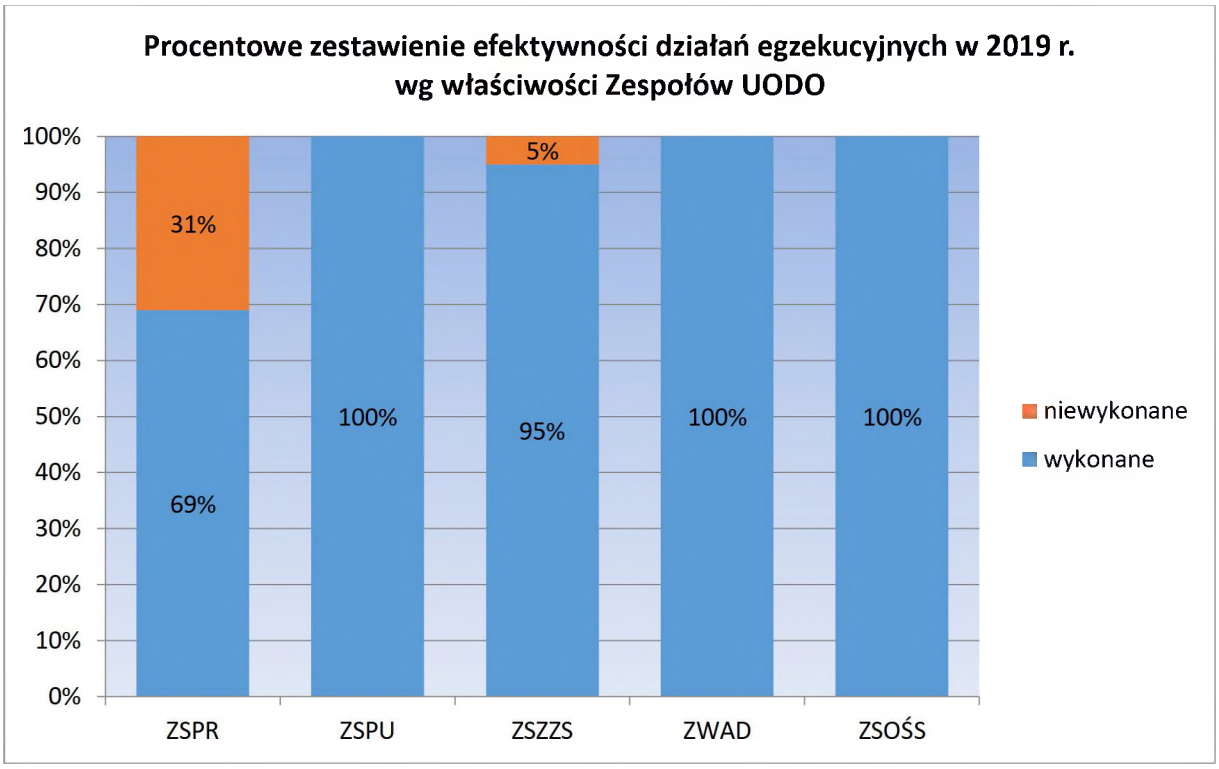
Wykres 2: Procentowe zestawienie rodzajów decyzji administracyjnych podlegających egzekucji wg właściwości komórek organizacyjnych UODO.

Efektywność działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków w 2019 r. przedstawia się następująco: spośród 118 decyzji **wykonanych zostało przez zobowiązanych 108 decyzji**, natomiast 10 decyzji pozostało niewykonanych. Decyzje te w dalszym ciągu objęte są działaniami egzekucyjnymi.

Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych przekazanych do egzekucji w 2019 r. wynosił **92 %**. W odniesieniu do właściwości komórek organizacyjnych UODO efektywność egzekucji przedstawia się następująco: **100 %** wobec decyzji leżących we właściwości Zespołów: ds. Sektora Publicznego, ds. Organów Ścigania i Sądów oraz Współpracy z Administratorami Danych, **95 %** wobec decyzji należących do właściwości Zespołu ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa, **69 %** wobec decyzji leżących we właściwości Zespołu ds. Sektora Prywatnego (zob. *Wykres 3 i Wykres 4).*

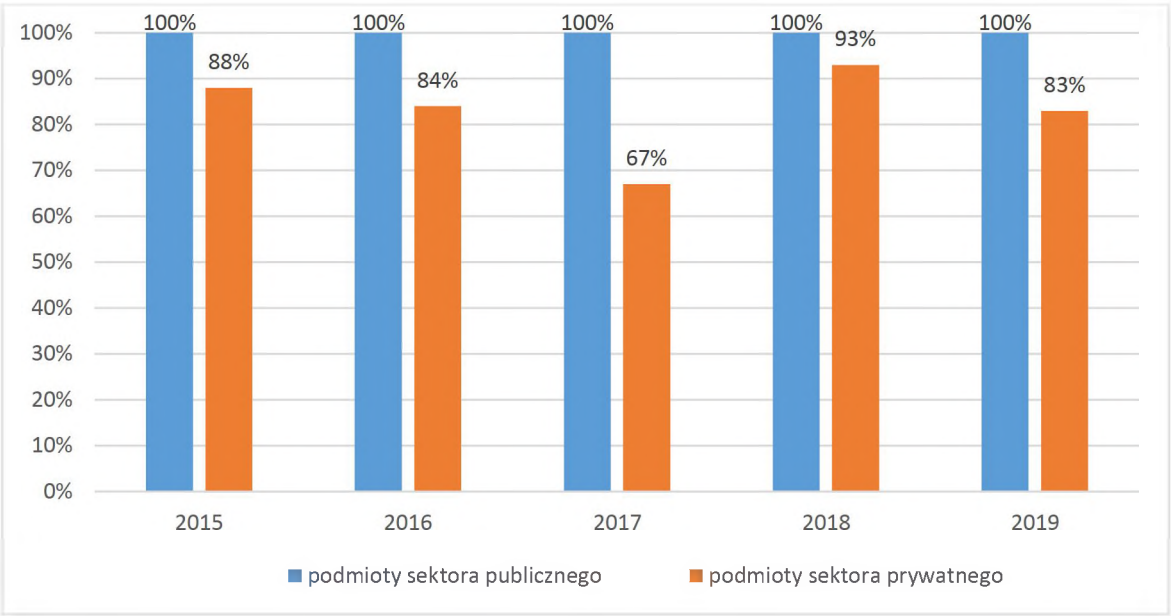


***Wykres 3*:** Liczbowe zestawienie efektywności działań egzekucyjnych w odniesieniu do rodzajów decyzji administracyjnych przekazanych do egzekucji w 2019 r.



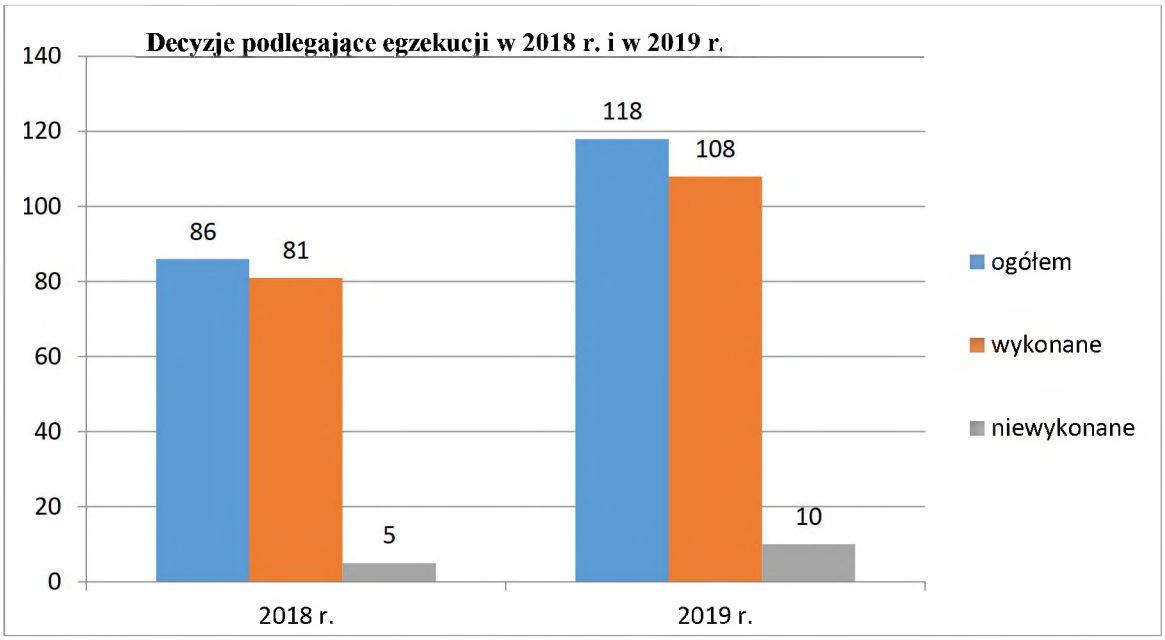
***Wykres 4*:** Procentowe zestawienie efektywności działań egzekucyjnych w odniesieniu do właściwości Zespołów UODO prowadzonych w 2019 r.

Działania egzekucyjne podejmowane w 2019 r. dotyczyły decyzji skierowanych w 50 % przypadków do podmiotów z sektora publicznego oraz w 50 % przypadków do podmiotów z sektora prywatnego. Wszystkie niewykonane decyzje dotyczą podmiotów z sektora prywatnego. Analizując na przestrzeni kilku lat efektywność działań egzekucyjnych organu ze względu na przynależność zobowiązanych do sektora publicznego i sektora prywatnego (zob. *Wykres 5*) to w latach 2015 – 2019 można zaobserwować w odniesieniu do podmiotów publicznych trend polegający na stale utrzymującej się 100% efektywności.

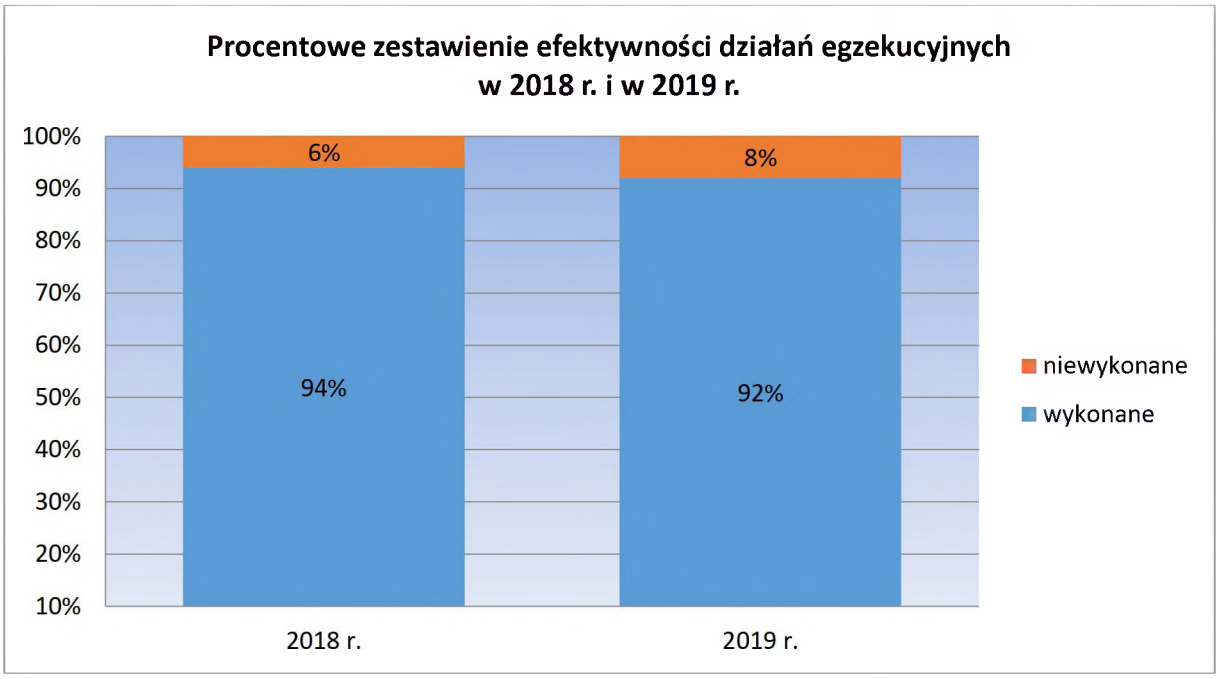


Wykres 5: Zestawienie efektywności prowadzonych działań egzekucyjnych w odniesieniu do podmiotów z sektora publicznego i sektora prywatnego w latach 2015 – 2019.

Porównując efektywność działań egzekucyjnych organu prowadzonych w 2019 r. do działań prowadzonych w roku 2018, można zauważyć, że pomimo tego, iż w 2019 r. przekazano do egzekucji o ponad 37% więcej decyzji niż w roku 2018, udało się zachować wysoki poziom efektywności działań, który w obu porównywanych okresach przekroczył **90 %** (*Wykresy 6 i 7*).



Wykres 6: Zestawienie decyzji UODO podlegających egzekucji administracyjnej i efektywność podejmowanych działań w 2018 r. oraz w 2019 r.



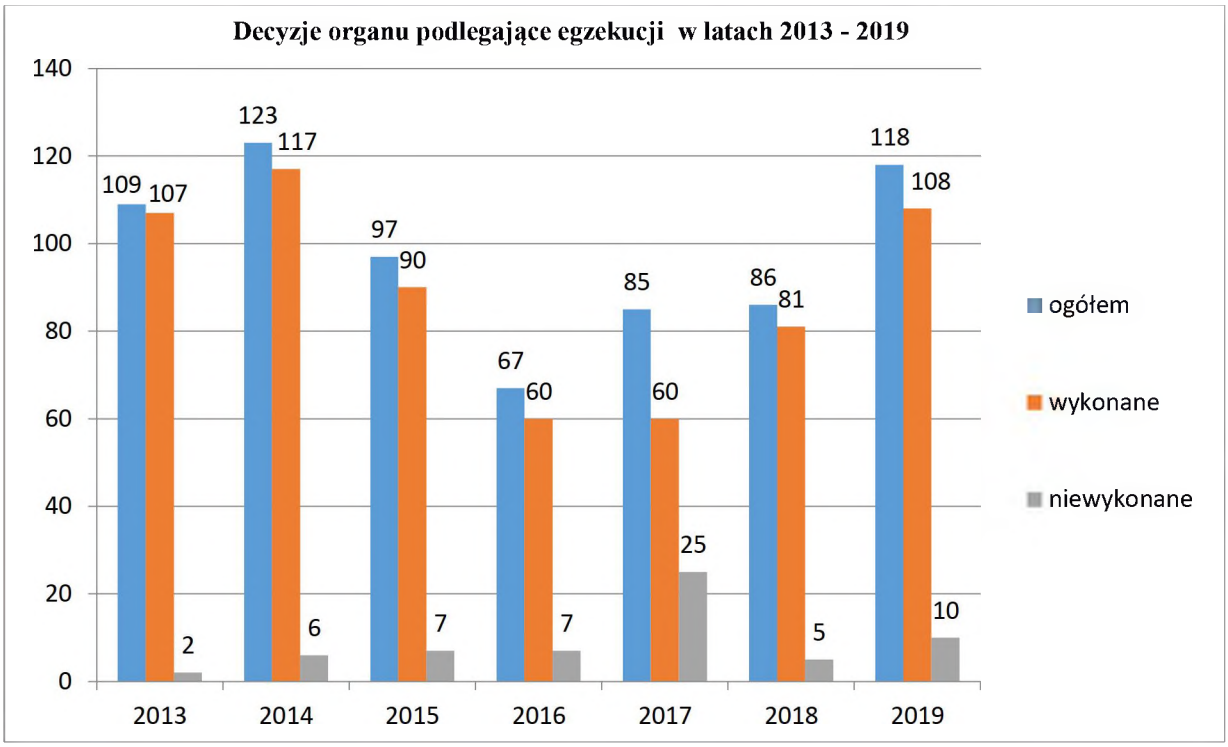
Wykres 7: Zestawienie procentowej efektywności działań egzekucyjnych organu nadzorczego w 2018 r. oraz w 2019 r.

Poniżej – zestawienie oraz *Wykres 8* przedstawiające liczbę decyzji przekazywanych do egzekucji od momentu powstania komórki egzekucyjnej w Urzędzie Ochrony Danych Osobowych:

- w 2013 r. przekazano 109 decyzji;

- w 2014 r. wpłynęły 123 decyzje, co stanowi wzrost o 13 % w stosunku do roku poprzedniego,
- w 2015 r. wpłynęło 97 decyzji administracyjnych, co stanowi spadek o 21% w stosunku do roku poprzedniego,
- w 2016 r. odnotowano wpływ 67 decyzji administracyjnych, co stanowi spadek o 31 %w stosunku do roku poprzedzającego,
- w 2017 wpłynęło 85 decyzji, co stanowi wzrost o 27 % w stosunku do roku poprzedzającego,
- w roku 2018 do egzekucji przekazano 86 decyzji, co przełożyło się na niewielki, bo 1 % wzrost w stosunku do roku poprzedniego,
- w 2019 roku do komórki egzekucyjnej wpłynęło 118 decyzji, co stanowi wzrost o 37 %w stosunku do roku ubiegłego.

Jak wynika z powyższego omówienia, od roku 2017 można zaobserwować tendencję wzrostową w stosunku do liczby decyzji przekazywanych do egzekucji. Duży wzrost decyzji, wobec których prowadzone były działania egzekucyjne w 2019 r. należy wiązać z intensyfikacją pracy Urzędu, która następowała po 25 maja 2018 r. w związku z rozpoczęciem stosowania nowych przepisów ochronie danych osobowych.



Wykres 8: Zestawienie decyzji organu nadzorczego podlegających egzekucji administracyjnej oraz efektywność podejmowanych działań egzekucyjnych w latach 2013 – 2019.

Natomiast procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych Generalnego Inspektora i Prezesa Urzędu wydanych w latach 2013–2019 przedstawia się następująco:

- w 2013 r. efektywność egzekucji wyniosła **98 %**,
- w 2014 r. efektywność egzekucji wyniosła **96 %**,
- w 2015 r. efektywność egzekucji wyniosła **93 %**,
- w 2016 r. efektywność egzekucji wyniosła **90 %**,
- w 2017 r. efektywność działań egzekucyjnych wyniosła **71 %**,
- w 2018 r. efektywność działań egzekucyjnych wyniosła **94 %**,
- w 2019 r. efektywność działań egzekucyjnych wyniosła **92 %**.

7. 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. Na gruncie art. 51 ustawy z 10 maja 2018 r. o ochronie danych osobowych, założenia i projekty aktów prawnych dotyczących danych osobowych są przedstawiane do zaopiniowania Prezesowi UODO.

Zadanie to realizowane jest poprzez analizę proponowanych zmian przepisów lub nowego ich brzmienia, pod kątem zgodności z przepisami rozporządzenia 2016/679 oraz ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Propozycje te badane są pod względem m.in. stworzenia właściwych podstaw przetwarzania danych, zakresów danych podlegających przetwarzaniu oraz celów tego przetwarzania. Istotne jest, czy projektodawca dokonał analizy wpływu przyjmowanych w przepisach rozwiązań na prywatność osób, których dane dotyczą. Analizowane są procesy i sposoby przetwarzania danych, udział podmiotów/organów w tych procesach, okresy retencji danych oraz to, 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 konieczność tworzenia rozwiązań zgodnych z przepisami, przyjaznych dla podmiotów stosujących prawo, tj. administratorów czy podmiotów przetwarzających, zarówno z sektora publicznego, jak i prywatnego, a także uwzględniających prawa osób, których dane osobowe są przetwarzane, na potrzeby publiczne czy prywatne.

Przedmiotem szczególnego zainteresowania organu nadzorczego były takie zagadnienia, jak: tworzenie nowych rejestrów publicznych, wywiązanie się przez projektodawców z obowiązku przeprowadzenia oceny skutków dla ochrony danych, projektowanie nowych rozwiązań cyfrowych ingerujących w prywatność osób, ochrona krajowego numeru identyfikacyjnego – PESEL, monitoring wizyjny czy przetwarzanie szczególnych kategorii danych.

W analizowanym 2019 roku zaopiniowanych zostało **691** projektów aktów prawnych.

Projekty aktów prawnych przedstawionych Prezesowi UODO w 2019 r. do zaopiniowania, dotyczyły różnorodnych zagadnień. Poniżej przedstawiono wybrane przykłady niektórych z nich.

Projekt ustawy z dnia 21 lutego 2019 r. ***o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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.***

Nowelizacje wielu ustaw mających zapewnić właściwe stosowanie RODO w polskim porządku prawnym były przedmiotem szczególnego zainteresowania organu nadzorczego. W dniu 4 maja 2019 r. zaczęła obowiązywać ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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). Ustawa wprowadza liczne zmiany w ustawodawstwie krajowym, obejmujące między innymi sektor ubezpieczeniowy oraz bankowy. I tak, istotną zmianą wprowadzoną do przepisów prawa bankowego w związku z postulatami Prezesa Urzędu Ochrony Danych Osobowych był nałożony przez ustawodawcę na banki obowiązek zapewniania osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymywania stosownych wyjaśnień, co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego

stanowiska[143]. Do innych bardzo istotnych kwestii regulowanych w tej ustawie zaliczyć można ograniczenia/wyłączenia w stosowaniu przepisów RODO, regulacje dotyczące monitoringu, określenie ról podmiotów w procesach przetwarzania danych osobowych oraz podstaw prawnych przetwarzania danych osobowych. W toku prac nad projektem Prezes UODO sygnalizował swoje wątpliwości, co do brzmienia przepisów poszczególnych ustaw. Projekt przewidywał wiele wyłączeń i ograniczeń obowiązków określonych w RODO. W wielu ustawach, w tym m.in. w ustawie Ordynacja podatkowa, pojawiły się propozycje wprowadzenia przepisów zakładających profilowanie. Organ nadzorczy wskazywał również, że RODO odstąpiło od konstrukcji pisemnych upoważnień do przetwarzania danych osobowych, które to rozwiązanie pojawiło się w wielu nowelizowanych ustawach. Uwagi Prezesa UODO częściowo zostały uwzględnione, jednak organ nadzorczy uznał, że ostateczny kształt wielu przepisów warto poddać ponownej analizie i dlatego ponowił zgłaszane na wcześniejszych etapach prac wciąż aktualne uwagi dotyczące następujących kwestii:

Zasada rozliczalności:

- **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**

  W opinii organu komentowana regulacja nie zapewnia ministrowi właściwemu do spraw informatyzacji kontroli nad procesem udostępnia danych z centralnej ewidencji wydanych i unieważnionych dokumentów paszportowych. 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 właściwych służb i organów.

Przetwarzanie szczególnych kategorii danych:

- **ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej**

[143] Art. 105a ust. 1a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. z 2018 r. poz. 2187 z późn. zm.).

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 negatywne stanowisko wobec upoważnienia służb statystyki publicznej do pozyskiwania danych genetycznych, wniósł o usunięcie z projektu uprawnienia służb statystyki publicznej do przetwarzania tak wysoce wrażliwej 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.

Zasada minimalizacji danych:

- **ustawa z dnia 23 maja 1991 r. o rozwiązywaniu sporów zbiorowych**

  Prezes UODO zaproponował rezygnację ze sformułowania „co najmniej", którego wprowadzenie skutkowałoby 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 celowe byłoby doprecyzowanie użytego w projekcie pojęcia „dane kontaktowe" poprzez wskazanie, jakie konkretnie dane wnioskodawcy (osoby ubiegającej się o przystąpienie do egzaminu) wchodzą w zakres tego pojęcia. Jego niedookreślenie może powodować, że zakres przetwarzanych danych osobowych będzie nadmierny w stosunku do celu, w którym będą one przetwarzane.

- **ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych**

Prezes UODO zwrócił uwagę na niejasność użytego przez projektodawcę pojęcia „dane kontaktowe" (osoby ubiegającej się o wydanie legitymacji lub jej duplikatu), w związku z czym zaproponował jego dookreślenie.

- **ustawa z dnia 27 października 1994 r. o autostradach płatnych oraz o 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 projektowany 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 miałyby 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.

Retencja danych:

- **ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej**
  Prezes UODO podał w wątpliwość stuletni okres przechowywania danych w Operacie do badań statystycznych.
- **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**
  Prezes UODO sprzeciwił się przewidzianemu okresowi przechowywania danych, zgodnie z którym w bazie danych o produktach i opakowaniach oraz o gospodarce odpadami, w przypadku dokumentów innych niż dokumenty ewidencji odpadów – dane osobowe będą przechowywane przez 100 lat, licząc od końca roku kalendarzowego, w którym zostały sporządzone te dokumenty.

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 tego rozwiązania 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 naraża projektodawcę na odpowiedzialność za uchwalenie przepisów prawa niezgodnych z elementarnymi zasadami RODO, 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 Ubezpieczeniowemu Funduszowi Gwarancyjnemu do podejmowania decyzji w indywidualnych przypadkach w oparciu

o zautomatyzowane przetwarzanie danych, w tym profilowanie, uznając przesłankę do profilowania za niewystarczającą. Prezes UODO podkreślił, że artykuł 22 ust. 2 lit. b RODO 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.

Wyłączenia stosowania RODO:

- **ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych**

  Prezes UODO wskazał, że przewidziane w nowelizacji ustawy wyłączenia stosowania RODO w odniesieniu do działalności Prezydenta RP są zbędne, gdyż przepisy RODO stosowane będą w tym przypadku bezpośrednio. Organ nadzorczy wskazał, że zapis ten jest nie tylko zbędny, lecz wręcz wprowadzający w błąd co do rzeczywistego zakresu stosowania przepisów RODO do działalności Prezydenta Rzeczypospolitej Polskiej.

Uprawnienia organu nadzorczego:

- **ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych**

  Prezes UODO podtrzymał wcześniej zgłaszane uwagi co do konieczności wyposażenia organu właściwego w sprawie ochrony danych osobowych w uprawnienie do występowania z wnioskiem do Sądu Najwyższego o rozstrzygnięcie zagadnienia prawnego, jeżeli w orzecznictwie sądów powszechnych ujawnią się rozbieżności w wykładni przepisów prawa dotyczących ochrony danych osobowych, oraz w uprawnienie do złożenia wniosku do Naczelnego Sądu Administracyjnego o podjęcie uchwały mającej na celu wyjaśnienie przepisów prawnych, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych. Organ nadzorczy wskazał również na konieczność wprowadzenia do ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych przepisów dotyczących rozstrzygania sporów kompetencyjnych między niezależnym organem nadzorczym a innymi organami administracji publicznej.

W projekcie ustawy ***o Krajowym Rejestrze Cudzoziemców***[144] Prezes UODO zwrócił uwagę na następujące kwestie istotne z punktu widzenia przetwarzania danych osobowych dotyczące przedmiotowej regulacji:

I. Rejestr Centralny

Przy tworzeniu przepisów dedykowanych systemom teleinformatycznym należy uwzględnić ochronę danych w fazie projektowania oraz domyślną ochronę danych (*Data protection by design and by default*, art. 25 RODO), a także ocenę skutków dla ochrony danych (*Data protection impact assessment*, art. 35 RODO). Konieczne jest też dysponowanie odpowiednimi podstawami do funkcjonowania systemów informatycznych w przepisach powszechnie obowiązującego prawa o właściwej ich randze. W kontekście art. 35 ust. 10 RODO Prezes UODO zwrócił uwagę na dokonanie oceny skutków dla ochrony danych już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej. Każdy system przetwarzania danych wykorzystujący mechanizmy teleinformatyczne wymagał będzie dogłębnej analizy w zakresie oceny wpływu, która powinna uwzględniać nie tylko wpływ zastosowanej technologii na ochronę danych osobowych osób, których dane mają być przetwarzane (art. 35 RODO), ale również interesy zaangażowanych stron z punktu widzenia transparentności wykonywanych operacji. Regulacje prawne – zwłaszcza w kontekście bliżej nieokreślonej planowanej „weryfikacji i identyfikacji cudzoziemców" – muszą nie tylko stanowić podstawę prawną przetwarzania danych, ale także precyzyjnie określać zakres danych osobowych (w formie katalogu zamkniętego) odpowiadający celom przetwarzania, podmioty przetwarzające te dane, cele, dla których dane będą przetwarzane oraz zasady ich przetwarzania (w tym retencji).

II. Odnosząc się do zakresu przetwarzanych danych osobowych Prezes UODO wskazał, że:

1) zaproponowany katalog przetwarzanych danych nie jest adekwatny do celu przetwarzania danych osobowych (nadmiarowe przetwarzanie danych różnego rodzaju);

2) numer PESEL stanowi „krajowy numer identyfikacyjny" w rozumieniu art. 87 RODO, co do którego powołany przepis rozporządzenia wprowadza dla państw członkowskich wymaganie, by jego przetwarzanie odbywało się z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą. Konieczne staje się przeprowadzenie oceny, czy zaproponowane rozwiązanie polegające na przetwarzaniu numerów PESEL cudzoziemców, nie stanowi nadmiernej i nieproporcjonalnej ingerencji w prawa i wolności osób, których dane mają się znaleźć

[144] ZSPR. 023.4.2019

w Krajowym Rejestrze Cudzoziemców. W świetle RODO identyfikator osoby musi być poddany szczególnej ochronie, w związku z czym należy stworzyć szczególne gwarancje wynikające z przepisów prawa, mając na względzie konieczność ich dostosowania do ww. rozporządzenia;

3) nadanie cudzoziemcowi numeru identyfikacyjnego określonego w projekcie ustawy jako „główny identyfikator cudzoziemca" (GIC) wymaga szczegółowego wyjaśnienia i uzasadnienia. Projektodawca tworząc nowe rozwiązania musi respektować zasady przetwarzania danych określone w rozporządzeniu: ograniczenie celu (art. 5 ust. 1 lit. b) oraz minimalizacji danych osobowych (art. 5 ust. 1 lit. c). Na Projektodawcy ciąży bowiem odpowiedzialność za ewentualne negatywne konsekwencje proponowanych unormowań, w tym również związane z możliwością naruszenia konstytucyjnie gwarantowanych praw i wolności człowieka i obywatela (m.in. prawa do ochrony danych osobowych – art. 51 Konstytucji RP).

III. W odniesieniu do przepisów projektu dotyczących administratora, Prezes UODO wskazał, że skoro to Komendant Główny Straży Granicznej został wskazany jako administrator, konieczne jest takie uregulowanie zasad przetwarzania danych osobowych w ramach krajowego rejestru, w którym to ten podmiot będzie decydował o celach i środkach przetwarzania danych osobowych (art. 4 pkt 7 RODO). Projekt zakłada „(...) prawo do pozyskania, weryfikacji lub uzupełnienia danych uzyskanych od cudzoziemca" przez określone podmioty, a zatem w kontekście art. 26 RODO, stanowiącego o współadministrowaniu, projektodawca powinien zastanowić się, czy planowane przetwarzanie danych nie będzie oznaczało współadministrowania danymi osobowymi, a jeśli tak, to powinien przewidzieć w projektowanych przepisach rozwiązania odpowiadające przepisom RODO regulującym współadministrowanie danymi osobowymi.

Z kolei do projektu ustawy ***o zmianie niektórych ustaw w celu ograniczenia obciążeń regulacyjnych***[145], Prezes Urzędu Ochrony Danych Osobowych zgłosił uwagi w zakresie propozycji zmian w ustawach: Prawo energetyczne, Prawo o sporcie. Zakwestionował też propozycję nowego brzmienia art. 69 pkt 1 projektu – art. 21a ustawy z dnia 6 marca 2018 r. – **Prawo przedsiębiorców,** w myśl którego *na przedsiębiorcę będącego: osobą fizyczną, mikroprzedsiębiorcą, małym przedsiębiorcą lub średnim przedsiębiorcą, który w okresie 12 miesięcy od dnia podjęcia działalności gospodarczej po raz pierwszy albo ponownie po upływie 36 miesięcy od dnia jej ostatniego zawieszenia lub zakończenia, naruszył przepisy prawa związane z wykonywaną działalnością w sposób uzasadniający wszczęcie postępowania mandatowego lub*

[145] ZSPR.023.21.2019

w sprawie nakładania lub wymierzania administracyjnej kary pieniężnej, postępowanie takie może zostać wszczęte tylko, jeżeli przedsiębiorca nie usunął stwierdzonych naruszeń w wyznaczonym przez organ terminie. W opinii organu propozycja ta jest niezgodna z przepisami RODO[146], które wyznaczają jego zadania i uprawnienia, a w art. 83 określają przesłanki nałożenia przez organ nadzorczy administracyjnej kary pieniężnej. Oczywistym jest, że – zgodnie z tymi przepisami – organ nadzorczy zastosuje je zależnie od okoliczności konkretnej sprawy, zwracając należytą uwagę w każdym indywidualnym przypadku na okoliczności, o których stanowi art. 83 RODO. Prezes UODO zaznaczył, że polski ustawodawca nie może tworzyć, w tym w przepisach o randze ustawy, podstaw warunkujących możliwość nałożenia kary pieniężnej za naruszenia związane z ochroną danych osobowych sprzecznych z prawem unijnym. Nie ma przy tym znaczenia, jak długo przedsiębiorca funkcjonuje na rynku, czy też w jakiej formie prowadzi działalność. Przedsiębiorca może bowiem prowadzić działalność gospodarczą krócej niż rok, być mikroprzedsiębiorcą, ale za to, np. przetwarzać gigantyczne zasoby danych osobowych albo szczególne kategorie danych. W przypadku incydentu w postaci wycieku takich danych, albo jakiegokolwiek innego działania (zaniechania) prowadzącego do niezgodnego z przepisami o ochronie danych osobowych ich przetwarzania, prawdopodobnym jest, że naruszenie takie będzie wypełniało przesłanki określone w art. 83 RODO i wymagało będzie nałożenia administracyjnej kary pieniężnej. Niezależny organ nadzorczy powinien zatem mieć swobodę w podjęciu indywidualnej decyzji, czy i z takiego uprawnienia skorzysta w konkretnej sprawie. Proponowany przepis mógłby stanowić zatem bezpodstawne ograniczenie przepisów RODO, a także generować problemy interpretacyjne tychże przepisów i ustawy Prawo przedsiębiorców.

Projektodawca nie uwzględnił uwag Prezesa Urzędu Ochrony Danych Osobowych w zakresie zmian w ustawie Prawo przedsiębiorców. Ustawa została uchwalona przez Sejm dnia 31 lipca 2019 r. i weszła w życie 1 stycznia 2020 .

Prezes Urzędu Ochrony Danych Osobowych brał udział także w rozpoczętych w 2018 r. pracach legislacyjnych nad projektem ustawy zmieniającej ustawę ***Prawo energetyczne***[147].

Wątpliwości Prezesa Urzędu wzbudziły przede wszystkim regulacje zakładające inteligentne opomiarowanie. Wskazał, że instalowane liczniki w mieszkaniach odbiorców energii posiadają zdolność dwustronnej komunikacji. Informują konsumentów o ilości zużywanej energii, przy czym informacja ta może być również przekazywana dostawcom energii i innym wyznaczonym

[146] zob. art. 57 i 58 RODO
[147] ZSPR.023.42.2018

podmiotom. Kluczową cechą inteligentnych liczników jest możliwość zdalnej komunikacji pomiędzy licznikiem i upoważnionymi podmiotami, takimi jak dostawcy, operatorzy sieci, upoważnione osoby trzecie lub przedsiębiorstwa usług energetycznych. Informacje zbierane od odbiorców końcowych przy pomocy liczników pozwalają zbudować profil użytkownika w zakresie ilości zużywanej energii i tym samym uzyskiwać szczegółowe informacje o jego zachowaniach. Podmioty, którym przekazywane są informacje z liczników mają wiedzę o tym, w jakich ilościach i kiedy użytkownik zużywa energię. Pozwala to na ustalenie, np. w jakich godzinach użytkownik pracuje, jak dużo posiada sprzętów elektrycznych, itd. Prezes wskazał na ryzyko profilowania użytkowników takich liczników, które w odstępach piętnastominutowych będą informowały dostawców o ilości i sposobach wykorzystywanej energii. Takie informacje pozwalają na stworzenie profilu osoby, jej zachowań, przyzwyczajeń, w jakich godzinach pracuje, kiedy, ile i na co zużywa energię elektryczną. Projektodawca przyjął, że celem stosowania liczników zdalnego odczytu nie jest profilowanie odbiorców końcowych, jakimi są gospodarstwa domowe. Jednakże ryzyko profilowania osób w związku z instalacją inteligentnych liczników w ocenie Prezesa UODO zdecydowanie zachodzi. Profilowanie nie musi być bowiem głównym celem działania systemu, może zaś zachodzić przy okazji jego użytkowania. Ponadto Prezes UODO nie zgodził się ze stwierdzeniem, że przy zastosowaniu inteligentnych liczników nie dochodzi do podejmowania zautomatyzowanych decyzji. Informacje gromadzone w ramach usługi inteligentnego pomiaru dotyczą profilu energetycznego konsumenta wynikającego z jego sposobu użytkowania energii i służą do podejmowania decyzji bezpośrednio go dotyczących. Taka decyzja w najbardziej oczywisty sposób dotyczy kształtowania poziomu opłat za dostawy energii, przy czym nie ogranicza się tylko do fakturowania. Prezes UODO wskazał, że projekt ten wymaga ponownej analizy i rozważenia wprowadzenia zmian w proponowanym przez niego zakresie. Wątpliwości Prezesa Urzędu Ochrony Danych Osobowych wzbudziła także propozycja określenia w przepisach ustawy Prawo energetyczne ustawowego współadministrowania danymi osobowymi w centralnym systemie informacji rynku energii.

Prezes Urzędu Ochrony Danych Osobowych zauważył, że projektodawca nie sformułował w przepisach wspólnych celów przetwarzania, dla jakich tworzy współadministrowanie. Organ nadzorczy podkreślił także, że ważne jest precyzyjne określenie w ustawie obowiązków każdego ze współadministratorów. W związku z uwagami zgłoszonymi przez Prezesa Urzędu Ochrony Danych Osobowych w projekcie ustawy doprecyzowane zostały obowiązki pomiędzy poszczególnymi współadministratorami. Odnosząc się do wątpliwości Prezesa Urzędu Ochrony Danych Osobowych w kwestii ryzyka związanego z profilowaniem w związku z regulacjami dotyczącymi

inteligentnego opomiarowania, projektodawca zauważył, że obowiązek wprowadzenia takich przepisów jest wymogiem wynikającym z regulacji unijnych. Organ nadzorczy wskazał, że rozumie konieczność wprowadzenia regulacji ze względu na obowiązek realizowania wymogów unijnych, oraz że dostrzega wiele korzyści, jakie z tego rozwiązania będą płynęły dla bezpieczeństwa energetycznego. Podkreślił jednak, że przepisy prawa powinny dawać gwarancję, że w związku z wprowadzeniem inteligentnych liczników nie będzie dochodziło do profilowania osób fizycznych. Zaznaczył, że jeżeli na obecnym etapie prac legislacyjnych wprowadzenie stosownych przepisów w tym zakresie nie jest możliwe, zasadnym jest, aby projektodawca rozważył wprowadzenie odpowiednich przepisów w przyszłości, jednakże przed rozpoczęciem stosowania inteligentnego opomiarowania, które zgodnie z projektem ma nastąpić w 2023 roku.

Prace nad projektem nie zostały jeszcze zakończone.

Stanowisko Prezesa UODO do *projektu* ***rozporządzenia Ministra Cyfryzacji w sprawie aplikacji mobilnej służącej do rozliczania opłaty za przewóz osób*** zawierało wskazanie, że projektodawca przy tworzeniu przepisów prawnych związanych z systemami teleinformatycznymi powinien pamiętać o uwzględnieniu ochrony danych w fazie projektowania oraz domyślnej ochrony danych (*Data protection by design and by default*, art. 25 RODO), a także oceny skutków dla ochrony danych (*Data protection impact assessment*, art. 35 RODO). W kontekście art. 35 ust. 10 RODO organ nadzorczy zwrócił uwagę na konieczność dokonania oceny skutków dla ochrony danych już w ramach oceny skutków regulacji. Każdy system przetwarzania danych wykorzystujący mechanizmy teleinformatyczne wymaga analizy w zakresie oceny wpływu, która powinna uwzględniać nie tylko wpływ zastosowanej technologii na ochronę danych osobowych osób, których dane mają być przetwarzane, o której mowa w art. 35 RODO, ale również interesy zaangażowanych stron z punktu widzenia transparentności wykonywanych operacji. Zgodnie z art. 35 ust. 1 RODO *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 (...).* Ocena skutków dla ochrony danych osobowych powinna zawierać co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje są niezbędne oraz

proporcjonalne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych. Projektodawca jest zobowiązany do dokonania analizy proponowanych przepisów w zakresie ich zgodności ze wskazaną wyżej zasadą. Zastrzeżenia organu nadzorczego wzbudził par. 2 pkt 2 przedmiotowego projektu rozporządzenia, który stanowi ogólnie o „gromadzeniu danych", bez szczegółowego wskazania, o jakie dane chodzi i czy w sformułowaniu tym mieszczą się także dane osobowe. Ponadto par. 3 pkt 2 stanowi o identyfikacji przewoźnika, kierowcy, klienta oraz innych osób biorących udział w realizacji usługi przewozu, natomiast projektodawca nie wskazuje, jakie dane identyfikacyjne miałyby być uwzględnione (brak katalogu przetwarzanych danych osobowych) oraz gdzie i przez kogo miałaby być wykonywana rejestracja tych danych (brak wskazania administratora danych). Organ nadzorczy wskazał również na par. 3 pkt 3 lit. e projektu i rejestrację incydentów uniemożliwiających realizację usługi przewozowej oraz niezbędność powiązania ich z osobami biorącymi udział w tych zdarzeniach – projektodawca w sposób ogólny, bez szczegółowego wyjaśnienia, nie wskazał jakie dane (i czy tylko klientów) będą przetwarzane w ramach rejestracji incydentów. Zdecydowany sprzeciw Prezesa UODO wzbudził par. 3 pkt 4 projektu rozporządzenia stanowiący o kontroli przez uprawnione podmioty, w dowolnym czasie, zarejestrowanych danych dotyczących realizowanej usługi. Nie wyjaśniono, jakie podmioty są uprawnione do przedmiotowej kontroli oraz na jakiej podstawie i w jakim zakresie. Brak uszczegółowienia tego bardzo ogólnego przepisu daje nieograniczony dostęp do danych osobowych nieokreślonym podmiotom/organom bez wskazania celu takiej kontroli, co jest niezgodne zarówno z przepisami o ochronie danych osobowych (motyw 31, art. 5 rozporządzenia 2016/679), jaki i narusza art. 51 ust. 1 i 2 Konstytucji RP.

Dnia 22 listopada 2019 r. Ministerstwo Cyfryzacji przekazało do zaopiniowania nowy projekt, który zasadniczo różnił się od wersji z 10 września 2019 r., pierwotnie opiniowanej przez Prezesa Urzędu Ochrony Danych Osobowych. Zrezygnowanie przez Ministra Cyfryzacji z wcześniej przyjętych w projekcie rozwiązań – w zakresie przetwarzania w aplikacji mobilnej danych szerokiego kręgu osób oraz dostępu do nich przez nieokreślone bliżej podmioty – zostało pozytywnie przyjęte przez organ nadzorczy, jako przykład realizacji zasady legalizmu oraz minimalizacji danych określonych w art. 5 ust. 1 lit. a i c RODO. Do tej wersji projektu Prezes Urzędu nie zgłosił zastrzeżeń.

Na etapie senackich prac nad ***projektem ustawy o narodowym spisie powszechnym ludności i mieszkań w 2021 r.***[148] Prezes UODO wskazał, że przewidziany stuletni okres przechowywania danych osobowych, które mają być zebrane w ramach narodowego spisu powszechnego ludności i mieszkań w 2021 wymaga analizy pod kątem zgodności z zasadą ograniczenia przechowywania wyrażoną w art. 5 ust. 1 lit. e RODO. Podczas narodowego spisu powszechnego ludności i mieszkań w 2021 r. mają być zbierane w szerokim zakresie dane osobowe, w tym również szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO (dane o niepełnosprawności i jej stopniu, czyli dane dotyczące zdrowia, dane o narodowości mogące ujawniać pochodzenie etniczne danej osoby oraz dane o wyznaniu).

Podobne uwagi zgłaszane były w czasie prac sejmowych nad projektem ***ustawy o powszechnym spisie rolnym w 2020 r.***[149] Projekt tej ustawy również przewidywał stuletni okres przechowywania danych osobowych, które mają być zebrane w powszechnym spisie rolnym w 2020 r., co w opinii organu wymaga rozważenia z uwzględnieniem zasady ograniczenia przechowywania wyrażonej w art. 5 ust. 1 lit. e RODO. Prezes UODO podkreślił jednocześnie, że w czasie powszechnego spisu rolnego w 2020 r. mają być zbierane dane osobowe w zakresie: imienia (imion) i nazwiska, daty urodzenia, płci, numeru PESEL, adresu zamieszkania lub pobytu, adresu do korespondencji, siedziby gospodarstwa rolnego, numeru telefonu stacjonarnego lub komórkowego oraz adresu poczty elektronicznej każdej osoby fizycznej będącej użytkownikiem gospodarstwa rolnego. Dlatego zaapelował, by raz jeszcze przeanalizować, czy ten bardzo obszerny zbiór danych osobowych rzeczywiście powinien być przechowywany przez Główny Urząd Statystyczny przez okres aż 100 lat od dnia zakończenia powszechnego spisu rolnego w 2020 r.

Opiniując projekt ***ustawy o realizowaniu usług społecznych przez centrum usług społecznych***[150], Prezes UODO wskazał, że program usług społecznych ma być udostępniany na stronie Biuletynu Informacji Publicznej urzędu gminy oraz na stronie Biuletynu Informacji Publicznej centrum usług społecznych. Program usług społecznych będzie więc jawny i powszechnie dostępny, co w kontekście art. 5 ust. 3 pkt 9 projektu stanowiącego, że program usług społecznych zawierał będzie dane osobowe niezbędne do kwalifikowania osób zainteresowanych do korzystania z usług społecznych określonych w programie, w tym dane osobowe, o których mowa w art. 9 ust. 1 i art. 10 RODO, budzi szczególne zaniepokojenie organu

[148] ZSPU.023.54.2018
[149] ZSPU.023.82.2018
[150] ZSPU.023.205.2018

nadzorczego. Są to bowiem dane szczególnej kategorii, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, jak również o wyrokach skazujących i naruszeniach prawa, których przetwarzanie powinno być poddane szczególnej ochronie. Organ nadzorczy zasygnalizował również kwestie retencji danych zawartych w programach usług społecznych. Wskazał, że projekt ustawy nie normuje, przez jaki okres dane osobowe zawarte w programie usług społecznych będą dostępne na stronach BIP. Prezes UODO zwrócił się również z wnioskiem o doprecyzowanie w projekcie, że sposób kontroli nad wykonaniem usług społecznych przekazanych do realizacji centrum, zawarty w porozumieniu, musi uwzględniać fakt, że będące jego stronami gminy są odrębnymi administratorami i jako takie mogą w czasie kontroli przetwarzać tylko te dane osobowe, co do których posiadają uprawnienia administratora. Organ nadzorczy zwrócił również uwagę na nieprecyzyjne unormowania dotyczące zakresu danych, które będą zawarte w diagnozach potrzeb i potencjału wspólnoty samorządowej w zakresie usług społecznych, a także na problem przetwarzania przez centra usług społecznych danych osobowych w związku z powoływaniem biegłych, prowadzeniem postępowań administracyjnych, uzyskiwaniem informacji od innych osób zgłaszających się do centrów, a niekorzystających z usług społecznych, które to przetwarzanie nie wynika wprost z projektu ustawy.

W 2019 r. Prezes UODO opiniował projekt ***ustawy o przejrzystości w zakresie zatrudniania osób bliskich w jednostkach sektora publicznego oraz o przeciwdziałaniu protekcji w naborze na stanowiska w jednostce sektora publicznego***[151]. Zwrócił uwagę, że na gruncie unormowań projektu ustawy, osoby zajmujące stanowiska w jednostkach sektora publicznego będą zobowiązane do składania oświadczenia zawierającego informacje o zatrudnieniu osób bliskich na podstawie umowy o pracę, mianowania, powołania lub umowy cywilnoprawnej w jednostce sektora publicznego. W związku z tym będą ujawniane dane osobowe osób bliskich dla osoby zobowiązanej dotyczące m.in. rodzaju relacji łączących osobę zobowiązaną z osobą bliską. Istnieje wysokie prawdopodobieństwo, że wśród tych danych znajdą się też dane dotyczące seksualności lub orientacji seksualnej, które to dane – zgodnie z art. 9 ust. 1 RODO – stanowią szczególną kategorię danych osobowych. Ujawnianie takich danych nie może naruszać istoty prawa do ochrony danych, muszą być również zapewnione odpowiednie i konkretne środki ochrony praw

[151] ZSPU.023.217.2018.OJ

podstawowych i interesów osoby, której dane dotyczą. Prezes UODO wskazał również na wiele innych zagadnień związanych z proponowanym kształtem ustawy. Zamieszczenie w oświadczeniu informacji o rodzaju relacji łączącej osobę zobowiązaną z osobą bliską prowadzi do przetwarzania danych osobowych, które nie są niezbędne do celów projektowanej ustawy, naruszając tym samym zasadę minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c RODO. Prezes UODO zwrócił uwagę, że w projekcie brak jest procedury pozwalającej dokonać sprostowania i uaktualnienia danych osobowych zawartych w oświadczeniach. Problematyczna jest też kwestia czasu przechowywania oświadczeń na stronach Biuletynu Informacji Publicznej, jak również obowiązku ujawniania informacji o pozostawaniu w relacji z osobami zobowiązanymi przez osoby starające się o zatrudnienie w jednostkach sektora publicznego. Prezes UODO zwrócił uwagę, że ujawnienie na podstawie przepisów projektu informacji o miejscu pracy, związkach rodzinnych lub osobistych, a także danych pozwalających określić seksualność lub orientację seksualną osoby, może naruszać art. 47 Konstytucji RP, który wskazuje, że każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Projekt ***ustawy o zmianie ustawy o odpadach oraz o zmianie niektórych innych ustaw***[152] był opiniowany przez Prezesa UODO na etapie komisji prawniczej. Nowelizacja zakładała utworzenie „Bazy danych o produktach i opakowaniach oraz o gospodarce odpadami (BDO)", której administratorem miałby być minister właściwy do spraw środowiska. Wątpliwości organu nadzorczego w ramach opiniowania projektu budziła możliwość powierzenia administrowania przez Ministra Środowiska innemu podmiotowi BDO w całości lub w określonym zakresie. Wynikało to z nieprecyzyjnych regulacji projektu ustawy w zakresie statusu administratora w związku z przewidzianymi w niej uprawnieniami ministra właściwego do spraw środowiska oraz marszałka województwa. Ocenie organu nadzorczego podlegała również zgodność projektu ustawy z art. 28 RODO, który warunkuje dopuszczalność powierzenia przetwarzania danych od istnienia odpowiedniego instrumentu prawnego.

Opracowany przez Ministra Cyfryzacji projekt ***ustawy o elektronizacji doręczeń oraz niektórych innych ustaw***[153] wzbudził wątpliwości Prezesa UODO, co do zasadności pozyskiwania na potrzeby prowadzenia bazy adresów elektronicznych, numeru PESEL osoby działającej w imieniu podmiotu publicznego. Numer PESEL to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy,

[152] ZSPU.023.7.2019
[153] ZSPU.023.42.2019

oznaczenie płci oraz liczbę kontrolną. Jest on ściśle powiązany ze sferą prywatną osoby fizycznej, nie zaś z jej czynnościami urzędowymi. Podlega również, jako krajowy numer identyfikacyjny, szczególnej ochronie na gruncie art. 87 RODO. Dlatego w ocenie organu nadzorczego, rozwiązanie dopuszczające przetwarzanie w bazie adresów elektronicznych numeru PESEL osoby działającej w imieniu podmiotu publicznego, wymaga analizy pod kątem zgodności z zasadą minimalizacji danych, o której mowa art. 5 ust. 1 lit. c RODO.

Prezes UODO zwrócił uwagę, że projekt ***ustawy o zmianie ustawy o dostępie do informacji publicznej***[154] w zakresie udostępniania informacji o wynagrodzeniach konkretnych osób zatrudnionych przez podmioty publiczne, odstępuje od kryterium pełnienia przez te osoby funkcji publicznych i zastępuje go „mechanicznym" kryterium wysokości wynagrodzenia (dwukrotność średniego miesięcznego wynagrodzenia ogłoszonego przez Prezesa Głównego Urzędu Statystycznego w Monitorze Polskim za rok ubiegły). Oznacza to, że zerwany zostaje związek pomiędzy wkroczeniem w sferę prywatności danej osoby (takim wkroczeniem jest podanie do publicznej wiadomości informacji o jej wynagrodzeniu) a faktem posiadania przez tę osobę określonego władztwa decyzyjnego, które to władztwo uzasadniało ograniczenie jej prawa do prywatności. Wskazano, że projekt nie tylko zmienia ideę ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, której celem było zapewnienie obywatelom informacji ze sfery publicznej, a nie prywatnej, lecz w zakresie ograniczenia prawa do prywatności osób niepełniących funkcji publicznych narusza zasadę proporcjonalności statuowaną w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej. Prezes UODO zwrócił również uwagę, że tak daleko idące rozwiązania nie zostały jednoznacznie sprecyzowane w uzasadnieniu projektu, co stanowi naruszenie zasady ograniczenia celu oraz zasady minimalizacji danych, o których mowa w art. 5 ust. 1 lit. b i c RODO.

Opracowany przez Ministra Cyfryzacji projekt ***ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw***[155] zakładał utworzenie rejestru danych kontaktowych, które podmiotom wykonującym zadania publiczne mają ułatwić kontakt z osobą fizyczną poprzez przesłanie jej określonych informacji na jej adres poczty elektronicznej lub telefon. Organ nadzorczy dostrzegł proobywatelski i innowacyjny charakter projektu oraz zaaprobował unormowania dotyczące możliwości usunięcia przez osobę, której dane dotyczą, jej danych z rejestru danych kontaktowych. Niemniej do części projektowanych rozwiązań

[154] ZSPU.023.99.2019
[155] ZSPU.023.119.2019

Prezes UODO wyraził pewne zastrzeżenia. Wskazał m.in., że ustawa o informatyzacji nie jest aktem prawnym właściwym do statuowania rejestru służącego szeroko rozumianej ewidencji ludności. Podniósł, że regulacja ta zawiera generalne unormowania dotyczące prowadzenia w Polsce procesu informatyzacji, nie jest więc (i nie powinna być) samodzielną podstawą dla tworzenia i prowadzenia przez podmioty publiczne konkretnych baz danych i rejestrów. Unormowania takie powinny znaleźć się w ustawie z dnia 24 września 2010 r. o ewidencji ludności. Prezes UODO wskazał również, że koncepcja udostępniania danych z rejestru danych kontaktowych za pomocą urządzeń teletransmisji danych, po złożeniu jednorazowego uproszczonego wniosku, nie zapewnia ministrowi właściwemu do spraw informatyzacji jakiejkolwiek kontroli nad tym procesem. Rozwiązania te uniemożliwiają zatem ministrowi właściwemu do spraw informatyzacji realizację wymogu rozliczalności, o którym mowa w art. 5 ust. 2 RODO. Wątpliwości Prezesa UODO wzbudziła również możliwość udostępniania danych z rejestru danych kontaktowych innym, nieokreślonym podmiotom na podstawie porozumienia z ministrem właściwym do spraw informatyzacji. W opinii do projektu zasygnalizował, że rozwiązanie to narusza zasadę przejrzystości z art. 5 ust. 1 lit. a RODO.

Opiniując projekt ***rozporządzenia Ministra Finansów w sprawie wzoru imiennego upoważnienia do przeprowadzenia kontroli podatkowej***[156] Prezes UODO zwrócił uwagę na treść klauzuli informacyjnej stanowiącej część upoważnienia do przeprowadzenia kontroli podatkowej. Zaznaczył, że w ocenie organu nadzorczego, brak jest uzasadnienia dla wskazywania przez projektodawcę jako podstawy prawnej przetwarzania danych osobowych w związku z kontrolą podatkową art. 6 ust. 1 lit. e RODO, który stanowi, że przetwarzanie jest dozwolone, kiedy jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Realizując obowiązek informacyjny z art. 13 RODO, administrator nie może wprowadzać w błąd osoby, której dane dotyczą, co do jej praw wynikających z przepisów o ochronie danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych zwrócił uwagę, że na podstawie projektowanego art. 10 ust. 1a ***ustawy o zmianie ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne***[157] mają zostać ujawniane zarówno informacje dotyczące majątku osób fizycznych pełniących funkcje publiczne, jak również informacje dotyczące majątku ich małżonków niepełniących takich funkcji. Projekt w zakresie udostępniania informacji o majątku

[156] ZSPU.023.128.2019
[157] ZSPU.023.130.2019

odrębnym małżonka Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu, Marszałka Senatu, Prezesa Rady Ministrów, wicemarszałka Sejmu, wicemarszałka Senatu, wiceprezesa Rady Ministrów oraz ministra, zakłada obowiązek udostępnienia zawierających dane osobowe informacji dotyczących osób, które nie pełnią funkcji publicznych. W opinii do projektu tej ustawy Prezes UODO zasygnalizował, że rozwiązanie to budzi wątpliwości, co do zgodności z zasadami ograniczenia celu oraz minimalizacji danych, o których mowa w art. 5 ust. 1 lit. b i c RODO i nie jest uzasadnione konstytucyjnym prawem dostępu do informacji publicznej.

W opinii projektu ***rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo***[158], Prezes UODO wniósł o uzupełnienie wymagań dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa o normę PN-ISO/IEC 29151: 2019-01, która określa wytyczne dotyczące wdrożenia zabezpieczeń w celu spełnienia wymagań zidentyfikowanych w trakcie szacowania ryzyka i oceny skutków związanych z ochroną informacji o identyfikowalnych osobach oraz o normę ISO/IEC 27002, która określa wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądaniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Organ nadzorczy wskazał również, że podmioty, których obowiązki regulować będzie rozporządzenie, powinny być zobowiązane wprowadzić zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji zgodnie z oszacowanym ryzykiem. W ocenie Prezesa UODO niezbędne jest uzupełnienie uzasadnienia do projektu rozporządzenia poprzez wskazanie, że niezależnie od obowiązków nałożonych przez projekt na podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, muszą realizować obowiązki wynikające z RODO, w szczególności z art. 25 tego aktu, tj. uwzględnić ochronę danych i prywatności na każdym etapie funkcjonowania systemu, a więc także w fazie projektowania – *privacy by design*.

Opinia Prezesa UODO do ***ustawy o zmianie ustawy – Prawo bankowe oraz niektórych innych ustaw***[159] została wyrażona w ramach obowiązkowej oceny przez ministra właściwego do spraw instytucji finansowych funkcjonowania unormowań odnoszących się do problematyki tzw. „rachunków uśpionych". Zagadnienie to jest przedmiotem szczególnego zainteresowania organu

[158] ZSPU.023.140.2019
[159] ZSPU.023.173.2019

właściwego w sprawie ochrony danych osobowych – w sprawie rachunków uśpionych kierowane były już do Ministra Finansów wystąpienia oraz uwagi w ramach opiniowania aktów prawnych dotyczących tego zagadnienia. Prezes UODO ponownie zwrócił uwagę, że obowiązujące przepisy ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe i ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, nakładają na banki i spółdzielcze kasy oszczędnościowo-kredytowe obowiązek przekazywania gminom szeregu informacji objętych tajemnicą bankową albo tajemnicą zawodową, w tym również danych osobowych, których przetwarzanie przez gminy nie znajduje uzasadnienia. Organ nadzorczy wskazywał, że obowiązek przekazywania przez banki i spółdzielcze kasy oszczędnościowo-kredytowe gminom informacji o posiadaczu rachunku dotyczy zarówno przypadku rozwiązania umowy rachunku z powodu śmierci posiadacza rachunku bankowego, jak i wygaśnięcia umowy rachunku ze względu na długotrwały brak aktywności posiadacza tego rachunku. O ile przekazywanie gminie informacji w przypadku śmierci posiadacza rachunku można uznać za uzasadnione, gdyż gmina może stać się spadkobiercą koniecznym takiego posiadacza, o tyle w przypadku wygaśnięcia umowy przekazywanie przez banki i spółdzielcze kasy oszczędnościowo-kredytowe gminie jakichkolwiek informacji o posiadaczu takiego rachunku nie wydaje się prawidłowe, gdyż nie ma podstaw do stwierdzenia, że posiadacz rachunku zmarł, a zatem gmina nie jest w takiej sytuacji nawet potencjalnym spadkobiercą. Nawet w sytuacji, kiedy Prezes UODO uznaje za dopuszczalne przekazywanie gminom tego typu informacji, to ich zakres wydaje się zbyt szeroki. O ile bowiem sama informacja o śmierci posiadacza rachunku (członka spółdzielczej kasy oszczędnościowo-kredytowej) może być gminie potrzebna do przeprowadzenia postępowania spadkowego, to – w ocenie organu właściwego w sprawie ochrony danych osobowych – brak jest podstaw, by informować gminę o dacie wydania przez posiadacza rachunku (członka spółdzielczej kasy oszczędnościowo-kredytowej) ostatniej dyspozycji dotyczącej tego rachunku, wysokości środków pieniężnych zgromadzonych na rachunku oraz kwotach i tytułach wypłat dokonanych z rachunku, a także źródle i podstawie dokonanych ustaleń. Dodać przy tym należy, że ustawodawca nie dookreślił w przepisach, jaki okres wstecz powinna obejmować informacja o kwotach i tytułach wypłat dokonanych z rachunku. Powyższe rozwiązania budzą więc wątpliwości, jako naruszające zasadę minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO.

Dla wzmocnienia prawa do ochrony danych osobowych osoby poszkodowanej, Prezes UODO wniósł o zmodyfikowanie art. 37 ust. 2 pkt 1 ***projektu ustawy o Państwowej Komisji do spraw wyjaśniania przypadków czynności skierowanych przeciwko wolności seksualnej i obyczajności,***

wobec małoletniego poniżej lat 15[160], poprzez usunięcie sformułowania „dane osobowe osoby poszkodowanej" i wprowadzenie katalogu danych osobowych osoby poszkodowanej, które ma zawierać postanowienie Państwowej Komisji o wpisie w rejestrze[161] prowadzonym przez Komisję. Prezes Urzędu Ochrony Danych Osobowych zwrócił również uwagę, że imię ojca osoby wskazanej jako sprawca w aktach sprawy, przekazanych przez prokuratora albo właściwy sąd, w stosunku do której wydane zostało postanowienie Państwowej Komisji o wpisie w rejestrze, powinno być ujawniane w rejestrze prowadzonym przez Komisję, gdyż to nie rodzice sprawcy dopuścili się czynu uzasadniającego umieszczenie danych sprawcy w rejestrze prowadzonym przez Komisję (mającym charakter jawny i publiczny). Prezes UODO wskazał również, że zamieszczanie w rejestrze prowadzonym przez Komisję nazwiska rodowego sprawcy, może być uznane za niezgodne z zasadą minimalizacji danych, o której mowa w art. 5 ust. 1 lit. i c RODO.

W projekcie ***ustawy o zmianie ustawy o postępowaniu egzekucyjnym w administracji oraz niektórych innych ustaw***[162] Prezes UODO wyraził opinię, że o ile przetwarzanie imienia i nazwiska zobowiązanego w obwieszczeniu o licytacji publicznej, ogłoszeniu o przetargu ofert, obwieszczeniu o licytacji publicznej nieruchomości może być, biorąc pod uwagę cel tych czynności, uznane za adekwatne, to nieuzasadnione jest podawanie do publicznej wiadomości (niejako „przy okazji" obwieszczenia o licytacji publicznej i ogłoszenia o przetargu ofert) adresu zobowiązanego będącego osobą fizyczną. Takie upublicznienie adresu zobowiązanego będącego osobą fizyczną stanowi niewspółmierną ingerencję w jego prawo do ochrony danych osobowych i narusza zasadę minimalizacji danych ustanowioną w art. 5 ust. 1 lit. c RODO.

Prezes UODO zgłosił uwagę do przewidzianego w projekcie ***ustawy o zmianie ustawy o podatku akcyzowym oraz niektórych innych ustaw***[163], nieograniczonego trybu teletransmisji danych, w ramach którego Dyrektor Urzędu Żeglugi Śródlądowej w Szczecinie udostępniałby Szefowi Krajowej Administracji Skarbowej, dane z bazy danych statków. Przekazywanie danych w drodze teletransmisji bez formułowania warunków, w których miałaby ona przebiegać, mogłoby naruszać przepisy RODO (sprzeczność z motywem 31 RODO) i jednocześnie uniemożliwiałoby Dyrektorowi Urzędu Żeglugi Śródlądowej realizację skutecznej ochrony danych osobowych

[160] ZSPU.023.178.2019
[161] Jest to rejestr osób, w stosunku do których Państwowa Komisja do spraw wyjaśniania przypadków czynności skierowanych przeciwko wolności seksualnej i obyczajności, wobec małoletniego poniżej lat 15, wydała postanowienie o wpisie w Rejestrze.
[162] ZSPU.023.200.2019
[163] ZSPU.023.230.2019

i wywiązanie się z zasady rozliczalności ciążącej na nim jako administratorze. Dodatkowo organ nadzorczy zwrócił uwagę, że udostępnianie danych z bazy danych statków w drodze teletransmisji jest nowym rozwiązaniem technologicznym, które wymaga przeprowadzenia przez projektodawcę oceny skutków planowanych rozwiązań dla ochrony danych osobowych.

Opiniując projekt ***rozporządzenia Ministra Cyfryzacji w sprawie aplikacji mobilnej służącej do rozliczania opłaty za przewóz osób***[164] realizowanych w usługach przewozowych i taksówkowych oraz pozwalającego na kontrolę danych związanych z przejazdami, Prezes UODO wyraził zaniepokojenie, że regulacja ta nie określa ani kręgu uprawnionych podmiotów, które będą miały dostęp do tych danych, ani zakresu tych danych. Daje to nieokreślonej kategorii podmiotów (w tym służbom i inspekcjom) uprawnienie do dostępu do bardzo szczegółowych informacji o osobie korzystającej z usługi przewozowej bez określenia celów, jakim taka kontrola miałaby służyć. Stwarza to ryzyko przeprowadzania w dowolnym momencie kontroli operacyjnych, które nigdzie nie zostaną odnotowane. W ocenie Prezesa Urzędu taka regulacja wymaga przeanalizowania z uwzględnieniem art. 51 ust. 1 i 2 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby oraz stanowiącym, że władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż jest to niezbędne w demokratycznym państwie prawnym. Prezes UODO w piśmie do Ministra Cyfryzacji zwrócił też uwagę na inne projektowane przepisy tego rozporządzenia, które warto byłoby doprecyzować. Projekt rozporządzenia nie określa bowiem, jakie dane mają być gromadzone przez aplikację mobilną do rozliczeń przewozów. Nie wiadomo również, przy wykorzystaniu jakich danych będzie się odbywać identyfikacja klienta w aplikacji. Tak skonstruowane przepisy mogą prowadzić do naruszenia zasady przejrzystości określonej w art. 5 ust. 1 lit. a RODO. Prezes UODO zwrócił też uwagę, że wprowadzenie rozwiązań silnie ingerujących w prywatność powinno być poprzedzone oceną skutków dla ochrony danych. W tym przypadku projektodawca tego nie zrobił.

W wyniku zgłoszonych przez Prezesa UODO uwag odstąpiono od wcześniej przyjętych w projekcie rozwiązań – w zakresie przetwarzania w aplikacji mobilnej danych szerokiego kręgu osób oraz dostępu do nich przez nieokreślone bliżej podmioty. Stanowi to dobry przykład właściwej realizacji zasady legalizmu oraz minimalizacji danych określonych w RODO.

[164] ZSPU.023.231.2019

Inicjatorem projektu ***ustawy o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw***[165] było Ministerstwo Sprawiedliwości. W założeniu miała ona umożliwić automatyzację procesu udzielania informacji z Krajowego Rejestru Karnego (KRK) oraz wydawanie zaświadczeń z KRK w czasie rzeczywistym. Cele te miały zostać osiągnięte poprzez zastosowanie pieczęci elektronicznej do wydawania zaświadczeń. Dotychczas jedynym sposobem skutecznego wydania zaświadczenia w formie elektronicznej było opatrzenie go kwalifikowanym podpisem elektronicznym. Projekt zakładał nadanie nowego brzmienia art. 217 § 4 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Zgodnie z projektowanym przepisem zaświadczenie w formie dokumentu elektronicznego może być opatrywane kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Organ nadzorczy pozytywnie odniósł się do inicjatyw upowszechniających użycie pieczęci elektronicznej. Kwalifikowana pieczęć elektroniczna jest narzędziem przypisanym podmiotowi nie zaś konkretnej osobie fizycznej. Oprócz nazwy podmiotu i jego danych weryfikacyjnych, takich jak numer NIP i numer REGON, zawarte są w niej dane osób reprezentujących określoną jednostkę organizacyjną podmiotu, którego pieczęć dotyczy, ale bez danej o tak szczególnym charakterze, jaką jest numer PESEL. Niestety, projektodawca założył również umożliwienie wydawania zaświadczeń przy pomocy podpisu zaufanego (używany do składania podpisów za pośrednictwem platformy ePUAP) oraz podpisu osobistego (podpis elektroniczny, który będzie można składać dowodem osobistym zawierającym warstwę cyfrową). Certyfikaty zarówno podpisu osobistego, jak i podpisu zaufanego, obligatoryjnie zawierają numer PESEL (w przypadku kwalifikowanego podpisu elektronicznego numer PESEL jest jednym z dopuszczalnych identyfikatorów i może być w nim umieszczany fakultatywnie). Konsekwencją tego jest możliwość odczytania numeru PESEL osoby, która podpisała dokument, przez każdego, kto weryfikuje ważność podpisu (w większości przypadków jest to prosta czynność techniczna dostępna przy pomocy standardowego oprogramowania). Konstrukcja projektowanego art. 217 § 4 k.p.a., która w równoważny sposób traktuje kwalifikowany podpis elektroniczny, pieczęć elektroniczną, podpis zaufany oraz podpis osobisty, może doprowadzić do sytuacji, w której organy administracji publicznej, zamiast wydawać swoim pracownikom kwalifikowane podpisy elektroniczne albo pieczęcie elektroniczne (narzędzia te są odpłatne), w celu wydawania zaświadczeń zaczną wymagać od nich posługiwania się podpisem zaufanym i podpisem osobistym.

[165] ZSPU.023.206.2019

W przypadku tych dwóch narzędzi nie ma możliwości wyłączenia numeru PESEL z certyfikatu podpisu, co stwarza zagrożenie dla prywatności osób, które będą zobligowane do posługiwania się nimi, nie życząc sobie jednocześnie ujawniania ich numerów PESEL.

Rodzi się również pytanie, czy w świetle obecnego brzmienia art. 22^1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy, pracodawca może wymagać od pracownika ujawniania swojego numeru PESEL poprzez podpisywanie dokumentów elektronicznych (w tym przypadku zaświadczeń). W ocenie organu nadzorczego równoważne potraktowanie kwalifikowanego podpisu elektronicznego, podpisu zaufanego, podpisu osobistego oraz kwalifikowanej pieczęci elektronicznej jest przykładem wykorzystania narzędzi cyfrowych do celów, dla których nie zostały stworzone. Wskazać tu można chociażby na art. 12d ust. 2 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, który wyraźnie wskazuje na domyślne zastosowanie podpisu osobistego w relacji pomiędzy osobą fizyczną a podmiotem publicznym, a w przypadku relacji pomiędzy osobą fizyczną a innym niż publiczny podmiotem – tylko pod warunkiem obustronnej zgody. Trudno sobie wyobrazić, by przy takiej konstrukcji skutku podpisu osobistego, pracownik podmiotu publicznego miał przy jego pomocy skutecznie wydać zaświadczenie (byłoby to teoretycznie możliwe przy wyrażeniu obustronnej zgody, ale byłaby to w swojej istocie zgoda wymuszona od pracownika podmiotu publicznego). Dlatego tak ważne jest przemyślane wprowadzanie nowych rozwiązań cyfrowych oraz wcześniejsza analiza ich wpływu na prywatność osób.

Projekt ***ustawy o Centralnej Informacji Emerytalnej***[166] zakłada utworzenie Centralnej Informacji Emerytalnej (CIE) – systemu teleinformatycznego zawierającego zintegrowane informacje emerytalne ze wszystkich filarów zabezpieczenia na starość. Opiniując tę ustawę, Prezes UODO uczulił projektodawcę – Ministra Rozwoju – iż w obecnym stanie prawnym konieczne jest przeprowadzenie oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Wynika to z rozmiaru projektowanej bazy danych, jak i faktu, że w ramach CIE będą podlegać łączeniu bazy danych: Zakładu Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego, funduszy emerytalnych, instytucji finansowych prowadzących indywidualne konta emerytalne, instytucji finansowych prowadzących indywidualne konta zabezpieczenia emerytalnego, podmiotów prowadzących rachunki uczestników pracowniczych programów emerytalnych, podmiotu prowadzącego Ewidencję Pracowniczych Planów Kapitałowych, organów emerytalnych określonych przez ministra właściwego do spraw wewnętrznych i Ministra Sprawiedliwości oraz

[166] ZSPU.023.258.2019.TG

wojskowych organów emerytalnych. Na konieczność przeprowadzenia oceny skutków dla ochrony danych w przypadku baz wielkoskalowych oraz łączenia danych z różnych rejestrów wskazują również pkt 7 i 8 załącznika do komunikatu Prezesa Urzędu Ochrony Danych Osobowych z 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony i – w przypadku operacji przetwarzania o dużej skali – motyw 91 RODO. W polu zainteresowania Prezesa UODO znalazła się też kwestia retencji danych osób, których dane będą ujęte w bazie; zagadnienie powierzania w drodze umowy wykonywania obsługi technicznej systemu CIE przez podmioty prywatne oraz ewentualnego podpowierzenia tej usługi. Przedmiotem uwag Prezesa UODO był również sposób realizacji obowiązku informacyjnego z art. 13 i 14 RODO, jak również zagadnienie upoważnień do przetwarzania danych osobowych w ramach CIE. Ustawa o Centralnej Informacji Emerytalnej jest przedmiotem szczególnego zainteresowania organu nadzorczego i będzie monitorowana przez organ nadzorczy na dalszych etapach procesu legislacyjnego.

Poniżej przedstawione zostały wybrane projekty aktów prawnych przesłanych przez **Ministerstwo Zdrowia** celem zaopiniowania ich przez organ właściwy do spraw ochrony danych osobowych.

W przypadku większości przedłożonych w 2019 roku przez Ministerstwo Zdrowia aktów prawnych, nie dokonano w nich oceny skutków planowanych operacji dla ochrony danych osobowych, który to obowiązek reguluje art. 35 ust. 1 w związku z ust. 10 RODO. Zgodnie z art. 35 ust. 7 RODO, ocena skutków zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje są niezbędne oraz proporcjonalne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych. Tymczasem przeprowadzenie oceny skutków projektowanej regulacji i zawarcie w tej regulacji lub w uzasadnieniu do niej informacji wskazanych w art. 35 ust. 7 RODO, ma istotne znaczenie dla prawidłowej oceny zaproponowanych przez projektodawcę uregulowań. Poprawnie przeprowadzona ocena skutków powinna wskazywać związek pomiędzy pozyskiwanym lub przekazywanym przez podmiot określony w ustawie zakresem danych, z konkretnym celem ich przetwarzania, który to cel również został wskazany w przepisach prawa powszechnie obowiązującego. Ocena skutków dla ochrony danych przeprowadzona na etapie projektowania przepisów w kontekście niezbędności przetwarzania danych powinna wskazywać, jako jeden z jej elementów, na zakres danych

niezbędnych do tego przetwarzania. Dopiero analiza przepisów szczegółowych, na podstawie których podmioty wskazywane w ustawie realizują swoje uprawnienia i w ramach tych zadań przetwarzają dane, pozwoli na dokonanie oceny przez projektodawcę i organ ochrony danych, czy dane powinny być przekazywane pomiędzy podmiotami w zaproponowanym zakresie oraz czy ten zakres jest wystarczający i niezbędny. Ma to znacznie z punktu widzenia zasad przetwarzania danych osobowych określonych w art. 5 ust. 1 RODO, w szczególności zasady ograniczenia celu i minimalizacji danych. Wskazanie w przepisach danych adekwatnych do celów sprawi, że regulacje te nie będą budziły wątpliwości interpretacyjnych. Ma to istotne znaczenie dla prawidłowej oceny zaproponowanych przez projektodawcę uregulowań.

Opiniowany przez Prezesa Urzędu Ochrony Danych Osobowych ***projekt rozporządzenia Ministra Zdrowia w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą***[167] przewidywał m.in. możliwość zainstalowania w pokojach pacjentów urządzeń umożliwiających ich obserwację w celu zapewnienia ich bezpieczeństwa w procesie leczenia.

Zastrzeżenia organu ochrony danych osobowych do projektowanych przepisów rozporządzenia dotyczyły braku przeprowadzonej przez projektodawcę analizy niezbędności korzystania przez placówkę z urządzeń monitorujących pacjentów i zaniechania szukania innych, równie skutecznych rozwiązań. Prezes UODO wskazał, że przetwarzanie danych za pośrednictwem kamer stwarza ryzyko przetwarzania danych osobowych innych osób biorących udział w procesie leczenia i udzielania świadczeń zdrowotnych, tj. osób przypadkowych, które mogą znaleźć się w polu działania kamery. Takie przetwarzanie jest niezgodne z zasadami określonymi w art. 5 ust. 1 RODO, w szczególności z zasadą minimalizacji danych (lit. c), zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celów przetwarzania. W ocenie Prezesa UODO wyrażony w § 29 projektu cel, tj. niezbędność w procesie leczenia oraz zapewnienie bezpieczeństwa pacjentów, są pojęciami niedookreślonymi, zbyt szerokimi i niejasnymi. Użyte przez projektodawcę pojęcie monitoringu nie rozwiewa również wątpliwości związanych z rodzajem prowadzonej obserwacji pacjenta, czy będzie to jedynie obraz, czy obraz i dźwięk.

[167] ZSZZS.023.26.2019

Opiniując ***projekt ustawy o zawodzie ratownika medycznego oraz samorządzie ratowników medycznych***[168] Prezes Urzędu Ochrony Danych Osobowych wnioskował, aby ustawodawca przeprowadził ocenę skutków dla ochrony danych, ponieważ ma ona istotne znaczenie dla prawidłowej oceny zaproponowanych przez projektodawcę uregulowań. Tworzenie przepisów bez przeprowadzonej dokładnej oceny skutków dla ochrony danych może prowadzić do braku podstawy prawnej przetwarzania danych osobowych przez podmioty wykonujące operacje na tych danych. Organ ochrony danych osobowych odniósł się również m.in. do kwestii nagrywania dźwięku, wskazując, że ze względu na swój inwazyjny charakter nagrywanie dźwięku, co do zasady, w systemach monitoringu nie powinno mieć miejsca. Takie uprawnienia posiadają jedynie służby porządkowe i specjalne na podstawie ustaw regulujących ich działalność. W ocenie organu ochrony danych zastosowanie rejestracji dźwięku w sytuacjach wskazanych przez projektodawcę, uznać należy za nadmiarową formę przetwarzania danych. Dla przetwarzania danych osobowych za pośrednictwem kamer, tj. monitoringu przestrzeni i osób oraz nagrywania i zapisywania zarejestrowanego obrazu, projektodawca powinien przeprowadzić obligatoryjnie ocenę skutków dla ochrony danych. Organ w swojej opinii wskazał również na konieczność dokonania zmiany przepisu dotyczącego przetwarzania w rejestrze ratowników informacji o przyczynie utraty przez nich prawa wykonywania zawodu, ponieważ informacja ta może dotyczyć danych o wyrokach skazujących i naruszeniach prawa, o których mowa w art. 10 RODO.

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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)[169] ***– w zakresie ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (wersja VIII)*** zakładał wyposażenie zespołów ratownictwa medycznego w kamery nasobne rejestrujące interwencje tych zespołów w celu zapewnienia im bezpieczeństwa.

Prezes UODO zakwestionował zastosowany tryb legislacyjny, ponieważ pominięto w nim mające istotne znaczenie z punktu widzenia praw jednostki i ochrony prywatności etapy uzgodnień, konsultacji publicznych i opiniowania. Ustawodawca nie dokonał też oceny skutków dla ochrony danych. Organ zwrócił także uwagę, że uzasadnienie do projektu ustawy nie zawierało informacji,

[168] ZSZZS.023.229.2019
[169] ZSZZS.023.21.2019

czy została rozważona możliwość wprowadzenia innych narzędzi, które realizowałyby przedstawiony cel, a jednocześnie mniej ingerowały w prywatność pacjentów oraz innych osób, które znalazłyby się w polu działania kamery. Prezes UODO wskazywał, że w trakcie nagrywania obrazu i dźwięku za pośrednictwem kamery nasobnej będzie dochodzić do ujawnienia tajemnicy lekarskiej oraz tajemnic zawodowych innych pracowników medycznych. Rejestrowanie interwencji zespołu ratownictwa medycznego w celach dowodowych będzie ingerencją w kompetencje organów ścigania uprawnionych do przeprowadzenia postępowania lub czynności wyjaśniających. Zakwestionował także spełnienie obowiązku informacyjnego względem osoby, której dane będą przetwarzane za pomocą kamery, poprzez podanie krótkiego słownego komunikatu „nagrywam".

Opiniowany przez Prezesa UODO ***projekt ustawy o zmianie niektórych ustaw w związku z wdrażaniem rozwiązań e-zdrowia***[170] przewidywał zmianę szeregu ustaw, w tym także aktów prawnych, do których organ do spraw ochrony danych osobowych zgłosił uwagi: ustawy o zawodach lekarza i lekarza dentysty, ustawy Prawo farmaceutyczne, ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawy o systemie informacji w ochronie zdrowia.

Prezes UODO zwrócił uwagę projektodawcy m.in. na konieczność doprecyzowania przepisów w kwestii upoważnienia asystentów medycznych do wystawiania dokumentów elektronicznej dokumentacji medycznej, a także doprecyzowania celu i okoliczności, w jakich farmaceuta będzie miał dostęp do dokumentacji medycznej. Zgłosił ponadto wątpliwość co do sposobu uregulowania przez projektodawcę przesłanki wyrażenia zgody na dostęp farmaceuty do danych osobowych i jednostkowych danych medycznych usługobiorcy. W projektowanej ustawie zaproponowano wprowadzenie przepisu, który kształtowałby uprawnienie dla Narodowego Funduszu Zdrowia, polegające na kierowaniu informacji z zakresu profilaktyki oraz zdrowego trybu życia bezpośrednio do pacjenta. Wzbudziło to niepokój Prezesa UODO z uwagi na fakt, że Narodowy Fundusz Zdrowia pozostaje płatnikiem, nie zaś świadczeniodawcą. Powyższa okoliczność rodzi pytania dotyczące charakteru oceny informacji o pacjencie i kierowanych na podstawie tej oceny komunikatów. Prezes UODO wskazywał również przepisy, w których brakowało postanowień dotyczących celu przetwarzania danych oraz nie zachowano zasady minimalizacji danych, a także wnioskował o wskazywanie wprost nazw systemów, do jakich będą przekazywane określone dane. Sygnalizował również, że projektodawca nie przedstawił oceny

[170] ZSZZS.023.75.2019

skutków planowanych operacji przetwarzania dla ochrony danych osobowych w rozumieniu art. 35 ust. 1 i ust. 10 RODO, pomimo iż zawarcie takich informacji w uzasadnieniu do projektowanej regulacji ma istotne znaczenie dla prawidłowej oceny zaproponowanych przez projektodawcę uregulowań.

W uwagach do ***projektu rozporządzenia Ministra Przedsiębiorczości i Technologii w sprawie sposobu i trybu sprawdzania kwalifikacji wymaganych przy obsłudze i konserwacji urządzeń technicznych oraz sposobu i trybu przedłużania okresu ważności zaświadczeń kwalifikacyjnych***[171], Prezes UODO wskazywał na nadmiarowe przetwarzanie danych w postaci numeru telefonu i adresu poczty elektronicznej osób fizycznych we wniosku o sprawdzenie kwalifikacji osób, o których mowa w art. 22 ust. 2 i 3 ustawy o dozorze technicznym, których podawanie powinno być dobrowolne. Zwrócił ponadto uwagę na brak podstawy prawnej do przetwarzania danych osobowych na formularzu wniosku wnioskodawcy innego niż osoba zainteresowana sprawdzaniem kwalifikacji, którym może być również pracodawca. W obowiązku informacyjnym dołączanym do wniosku Prezes UODO zarekomendował zmianę podstawy prawnej do przetwarzania danych osobowych z art. 6 ust. 1 lit. e na art. 6 ust. 1 lit. c RODO, argumentując zgłoszoną uwagę obowiązkiem przetwarzania danych, który wynika z konkretnego przepisu. Prezes UODO wnioskował także o doprecyzowanie czasu przetwarzania danych osób składających wniosek.

Prezes UODO w opinii *do* ***projektu rozporządzenia Ministra Kultury i Dziedzictwa Narodowego w sprawie badania jakości kształcenia artystycznego w publicznych szkołach artystycznych***[172] zakwestionował m.in. celowość przetwarzania danych uczniów wraz z uzyskaną oceną komisji zawartych w protokołach, mając na uwadze, że na ich podstawie tworzy się raporty wraz z wnioskami i rekomendacjami, czyli dokumenty o zbiorczym i ogólnym charakterze. Prezes UODO wskazywał, że wymóg celowości wynika przede wszystkim z zasad określonych w art. 5 RODO, w szczególności z zasady ograniczenia celu (lit. b) oraz minimalizacji danych (lit. c), zgodnie z którymi dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzane dalej w sposób niezgodny z tymi celami oraz adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

[171] ZSZZS.023.51.2019
[172] ZSZZS.023.59.2019

Opiniując ***projekt ustawy o zawodzie lekarza i lekarza dentysty***[173] Prezes UODO zakwestionował m.in. przepis, który stanowił, że przebieg udostępniania testów i pytań testowych egzaminów może być monitorowany za pomocą urządzeń rejestrujących obraz i dźwięk. W ocenie Prezesa UODO brzmienie tego przepisu pozostawiało pewną dowolność w zakresie przetwarzania danych w postaci dźwięku i obrazu oraz nie miało charakteru obligatoryjnego. Ponadto projektodawca nie określił czasu przechowywania nagrań, nie wskazał, jakie podmioty będą miały do nich dostęp, a sam cel wprowadzenia tej regulacji nie był jasno sformułowany. Prezes wskazał również, że administrator danych osobowych, zgodnie z art. 15 i następne RODO, jest zobowiązany realizować szereg obowiązków względem osoby, której dane dotyczą, m.in. prawo dostępu do danych. Zatem stosowanie urządzeń rejestrujących obraz i dźwięk będzie rodziło obowiązki administratora wskazane wprost w przepisach ogólnego rozporządzenia o ochronie danych.

Wątpliwości Prezesa UODO wzbudziła także przesłanka dotycząca nienagannej postawy etycznej osoby, której rada lekarska ma przyznać prawo wykonywania zawodu. W ocenie organu do spraw ochrony danych osobowych jest to termin nieostry i stanowiący zwrot niedookreślony, który odwołuje się do przesłanek uznaniowych o charakterze ocennym. Mając na uwadze zasadę minimalizacji danych, Prezes UODO odniósł się także do kwestii danych niezbędnych do identyfikacji danej osoby fizycznej, podnosząc, że dane w zakresie imion rodziców, daty i miejsca urodzenia oraz miejsca zameldowania lub aktualnego zamieszkania nie są niezbędne do potwierdzenia tożsamości lekarza. W związku z powyższym organ do spraw ochrony danych osobowych zawnioskował o usunięcie tych danych z treści projektu.

8. Zgłaszanie naruszeń ochrony danych osobowych

Zadaniem Urzędu realizowanym od 25 maja 2018 r. jest 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 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.

[173] ZSZZS.023.118.2019

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.

W celu zapewnienia należytego wywiązania się z tego obowiązku przez administratorów, Urząd Ochrony Danych Osobowych 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 jest mniejsze, niż w przypadku naruszeń przesyłanych przez administratorów bez jego użycia.

Niektóre zmiany w formularzu zostały wprowadzone przez UODO w związku z zacieśnieniem w kwietniu 2019 r. współpracy z Państwowym Instytutem Badawczym NASK – co było związane z rosnącą liczbą zgłoszeń naruszeń ochrony danych osobowych w wyniku np. działania złośliwego oprogramowania, łamania zabezpieczeń informatycznych czy oszustwami komputerowymi (takimi jak phishing). Wspólnym celem obu instytucji było wzmacnianie wymiany informacji o zagrożeniach dla danych osobowych i podejmowanie działań informacyjno-edukacyjnych w zakresie ochrony prywatności i bezpieczeństwa teleinformatycznego. Na skutek podjętych działań w formularzu zgłaszania naruszeń wprowadzone zostały pytania dotyczące działania złośliwego oprogramowania oraz zgłaszania zdarzeń i zagrożeń teleinformatycznych Zespołowi CERT Polska.

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. 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. Administrator ma obowiązek podjęcia skutecznych działań zapewniającym ochronę osobom fizycznym i ich danym osobowym.

W 2019 r. Urząd Ochrony Danych dokonał analizy **6039 zgłoszeń naruszeń** m.in. pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, **w tym 3894 zostało zgłoszonych przez podmioty sektora prywatnego, 2145 przez podmioty sektora publicznego, zaś 69 zgłoszonych w międzynarodowym systemie informatycznym (IMI).** W przypadku sektora prywatnego najwięcej zgłoszeń napłynęło od podmiotów: **telekomunikacyjnych (1433), ubezpieczeniowych (638), banków i podmiotów finansowych (527) oraz służby zdrowia (206).** W sektorze publicznym zawiadomienia o incydentach z danymi osobowymi najczęściej nadsyłały **jednostki samorządu terytorialnego (453), szkoły, przedszkola, żłobki (148) oraz placówki służby zdrowia (166).**

Dla porównania, w okresie 7 miesięcy – od 25 maja do 31 grudnia 2018 r. – UODO dokonał analizy **2446 zgłoszeń naruszeń** pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w tym **1882** naruszenia zostały zgłoszone przez podmioty sektora prywatnego, zaś **564** przez podmioty sektora publicznego.

Wzrost liczby zgłoszeń naruszeń ochrony danych osobowych w 2019 r. wynika z jednej strony z większej świadomości administratorów co do ich obowiązków wynikających z art. 33 oraz 34 rozporządzenia 2016/679, z drugiej – z obawy przed konsekwencjami, o których mowa w art. 58 oraz 83 ust. 4, 5 i 6 rozporządzenia 2016/679. W zgłoszeniach naruszeń przodują podmioty prywatne, w szczególności prowadzące działalność w sektorach telekomunikacyjnym, ubezpieczeniowym oraz finansowym. W przypadku podmiotów publicznych najczęściej zgłaszano naruszenia w jednostkach samorządu terytorialnego, placówkach oświaty oraz służby zdrowia. Wszystkie wyżej wymienione podmioty, w porównaniu do poprzedniego okresu sprawozdawczego, poprawiły procedury, szczególnie w aspekcie dokonywania analizy ryzyka naruszenia praw lub wolności osób fizycznych, jak również prawidłowego konstruowania zawiadomień o naruszeniu ochrony danych osobowych, zgodnie z art. 34 rozporządzenia 2016/679.

Rok 2019 był **pierwszym rokiem przyjmowania przez UODO zgłoszeń naruszeń ochrony danych od administratorów przetwarzających dane osobowe w związku z zapobieganiem i zwalczaniem przestępczości**. Od chwili wejścia w życie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, do Urzędu Ochrony Danych Osobowych zaczęły napływać zgłoszenia naruszeń na podstawie tych przepisów. Art. 44 ustawy nałożył na administratorów przetwarzających dane osobowe, w związku z zapobieganiem i zwalczaniem przestępczości, analogiczny obowiązek, jak na administratorów na podstawie art. 33 ust. 1 RODO, a w art. 45 ustawy na administratorów nałożono tożsamy obowiązek, jaki istnieje na gruncie art. 34 RODO, tj. obowiązek zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Przy czym od tego drugiego obowiązku przewidziano pewne wyjątki. Opóźnienie, ograniczenie bądź odstępstwo od tego obowiązku może mieć miejsce wyłącznie w przypadku, o którym mowa w art. 26 ust. 1 ustawy, tj. gdy przekazanie informacji mogłoby powodować: 1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych; 2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych; 3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe; 4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego; 5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa; 6) istotne naruszenie dóbr osobistych innych osób.

8.1. Sektor publiczny

Zgłoszenia naruszeń ochrony danych osobowych z sektora publicznego

W analizowanym 2019 r. Urząd Ochrony Danych Osobowych rozpatrywał **1042 zgłoszenia naruszeń** ochrony danych osobowych dotyczących sektora publicznego oraz sektora mieszkaniowego, w tym zarządców nieruchomości, którym zarząd wspólnoty mieszkaniowej powierzył zarządzanie nieruchomościami. Naruszenia z sektora mieszkalnictwa stanowiły około 10 procent wszystkich zgłaszanych naruszeń.

Zadaniem organu była analiza tych zgłoszeń głównie pod kątem środków i rozwiązań, które administrator deklarował zastosować w celu minimalizacji ryzyka ponownego wystąpienia naruszenia w przyszłości – czy są one wystarczające oraz czy zostały wdrożone. Gdy było to zasadne, organ nadzorczy podejmował odpowiednie działania służące zminimalizowaniu

wystąpienia naruszeń w przyszłości, np. kierował wystąpienia[174] bądź pisma z wnioskiem o uzupełnienie zgłoszenia lub udokumentowanie wdrożenia zadeklarowanych działań[175]. Naruszenia zgłaszane zarówno przez podmioty z sektora publicznego, jak i przez zarządy wspólnot mieszkaniowych w dużej mierze dotyczyły sytuacji, w których naruszone zostały dane pojedynczych osób, a tego typu przypadki zdarzały się w danej jednostce sporadycznie. W przypadku wspólnot były to najczęściej naruszenia dotyczące mieszkańców spowodowane wysyłaniem korespondencji dotyczącej rozliczeń należnych opłat, np. za zużycie wody czy prądu, pod niewłaściwy adres, zarówno poczty elektronicznej, jak i tradycyjny adres zamieszkania.

W sektorze publicznym do najczęściej zgłaszanych naruszeń należały:

1. *udostępnienie adresatowi korespondencji danych innej osoby na skutek nieprawidłowego zaadresowania bądź spakowania przesyłki* (zarówno tej tradycyjnej, jak i wysyłanej drogą elektroniczną); częstym błędem było kierowanie jednobrzmiącej, masowej korespondencji bez ukrycia adresów e-mail wszystkich adresatów wiadomości poprzez ich wpisywanie w pole „DO" zamiast w pole UDW, tj. „ukryte do wiadomości"; do naruszeń w tym obszarze dochodziło też na skutek pomyłki w adresie e-mail adresata z powodu jego błędnego wpisania w momencie wysyłki lub wprowadzenia niewłaściwych danych do sytemu informatycznego (np. wprowadzenie na koncie klienta adresu e-mail/adresu korespondencyjnego innego klienta) – w tym przypadku naruszenia powstawały najczęściej na skutek błędu pracowników i z reguły miały charakter incydentalny, zaś administratorzy podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia, dokonywali przeglądu procedur i wykonywali audyty bezpieczeństwa;
2. *udostępnienie w trybie dostępu do informacji publicznej, w tym w Biuletynie Informacji Publicznej, danych nieadekwatnych, nadmiarowych* – w tym przypadku powodem powstania naruszeń była najczęściej nieprawidłowa anonimizacja danych lub przeoczenie tego błędu przez pracowników udostępniających materiały, w tym zamieszczających je w sieci; środkami zaradczymi wdrażanymi przez administratorów były z reguły przeglądy i modyfikacja procedur udostępniania informacji publicznej, np. wprowadzenie dodatkowej weryfikacji anonimizacji dokumentów;
3. *udostępnienie danych osobowych osobie nieuprawnionej* – do tego rodzaju naruszenia dochodziło wskutek wydawania dokumentów (np. zaświadczeń) niewłaściwym osobom, co

[174] ZSPU.405.236.2019, DKN.405.56.2019.
[175] ZSPU.405.118.2018, ZSPU.405.90.2018, ZSPU.405.848.2019, ZSPU.405.614.2019.

najczęściej było spowodowane brakiem uprawnień osób zgłaszających się z wnioskiem o udostępnienie dokumentów czy danych; do podejmowanych przez administratorów działań niwelujących skutki naruszeń i mających im zapobiegać w przyszłości, należały dodatkowe szkolenia pracowników, przegląd i modyfikacja bądź opracowanie procedur udostępniania dokumentów lub danych z uwzględnieniem przepisów szczególnych, kontrola ważności upoważnień dostępu do dokumentów lub danych, zobowiązywanie osób, które na skutek pomyłki weszły w posiadanie danych osobowych osób trzecich do zwrotu lub zniszczenia zawierających je dokumentów;

4. *zniszczenie, kradzież dokumentacji bądź niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych (smartfonów, komputerów przenośnych, pendrive'ów) zawierających dane osobowe* – w tej kategorii wyróżnić można naruszenia polegające na zagubieniu korespondencji przez operatora pocztowego; w celu ich eliminacji administratorzy podejmowali działania mające na celu ustalenie przyczyn zagubienia korespondencji, składali reklamacje, podejmowali działania mające doprowadzić do weryfikacji umów zawartych z operatorem pocztowym. W przypadku kradzieży zawierających dane osobowe nośników elektronicznych lub dokumentów, administratorzy zgłaszali zdarzenia organom ścigania; jednocześnie wprowadzali obowiązek stosowania rozwiązań szyfrujących dane osobowe, a także umożliwiających zdalne usuwanie danych osobowych ze stacji roboczych znajdujących się poza siedzibą administratora;
5. *zagubienie przez pracowników dokumentów zawierających dane osobowe klientów* – do tego typu naruszeń dochodziło przede wszystkim w tych obszarach, w których praca polega na kontaktach z klientem w miejscu jego zamieszkania (np. agentów ubezpieczeniowych, doradców finansowych). W celu eliminowania tego typu naruszeń w przyszłości administratorzy zobowiązywali pracowników, by przy wyjazdach do klientów do niezbędnego minimum ograniczyli ilość zabieranej dokumentacji, nie wynosili poza siedzibę dokumentacji klientów, z którymi na dany dzień nie jest umówione spotkanie, a gdy to możliwe przewozili dokumentację w formie elektronicznej na zaszyfrowanych urządzeniach informatycznych.
6. *złamanie zabezpieczeń systemu informatycznego, które skutkowało zablokowaniem dostępu do plików, całego komputera lub wewnętrznej sieci intranetowej przez złośliwe*

oprogramowanie typu ransomware[176] – analizując tego typu zgłoszenia, organ nadzoru zwracał uwagę, czy zaatakowane podmioty dysponują kopią zapasową danych osobowych umożliwiającą przywrócenie pracy. Jeśli ich nie posiadały, to rozpoczęcie ich tworzenia było jednym z działań, które było podejmowane przez administratorów w celu wyeliminowania ryzyka zaistnienia podobnych zdarzeń w przyszłości. Do innych działań – stosowanych wówczas, gdy komputery miały połączenie z siecią internetową – należy zaliczyć zainstalowanie aktualnego oprogramowania antywirusowego oraz kontrolującego dostęp do komputera z zewnątrz (firewall). Ponadto administratorzy uczulali personel, by szczególną ostrożność zachował podczas użytkowania nieznanych urządzeń USB oraz przy otwieraniu załączników poczty elektronicznej.

Podsumowując ten obszar działalności wskazać można, że liczba zgłoszeń naruszeń przesyłanych przez podmioty z sektora publicznego maleje. Jest to spowodowane wprowadzaniem i udoskonalaniem przez nie polityk bezpieczeństwa, zasad postępowania z dokumentami zawierającymi dane osobowe, m.in zasady czystego biurka, jak również ciągłych szkoleń pracowników sektora publicznego z zakresu ochrony danych osobowych.

Niemniej istnieje pewna grupa podmiotów, w których nadal dochodzi do sporej liczby naruszeń, najczęściej związanych z dostarczaniem korespondencji i publikacją danych osobowych w Biuletynie Informacji Publicznej (BIP) lub na stronie internetowej. Są wśród nich: Zakład Ubezpieczeń Społecznych, izby administracji skarbowej, ministerstwa, urzędy gmin, miejskie ośrodki pomocy społecznej. Jest to spowodowane zarówno liczną korespondencją wysyłaną zarówno drogą tradycyjną, jak i elektroniczną, jak również koniecznością publikacji dużej ilości informacji w Biuletynie Informacji Publicznej. W takich sytuacjach często dochodziło do pomyłek pracowników – błędów w adresowaniu czy niewłaściwej anonimizacji dokumentów.

Osobnym problemem związanym z obowiązkiem zgłaszania naruszeń ochrony danych były konsekwencje związane z niewłaściwym dostarczaniem korespondencji przez narodowego operatora pocztowego, tj. Pocztę Polską S.A. Poczta Polska wykonuje bowiem obowiązki administratora w rozumieniu przepisów RODO wyłącznie w odniesieniu do takich danych, jak imiona, nazwiska i adresy osób, do których kierowana jest korespondencja. Administratorem danych osobowych zawartych w korespondencji pozostaje podmiot ją wysyłający. W przypadku zagubienia

[176] 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).

przesyłki jej nadawca nawet o tym nie wie i dlatego nie dokonuje oceny ryzyka naruszenia praw i wolności osób fizycznych, do których adresowana była korespondencja. W efekcie nie wie też, czy konieczne jest zawiadomienie osób, których dane zostały naruszone, oraz zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych osobowych. Zatem nadawcy korespondencji, zwłaszcza w sektorze publicznym, którzy w wielu przypadkach zobowiązani są do korzystania z usług narodowego operatora pocztowego, mimo iż nie mieli bezpośredniego wpływu na zaistniałe naruszenie, mają obowiązek przeanalizowania związanego z tym ryzyka i ewentualnego zgłoszenia naruszenia organowi nadzorczemu.

Niemniej wskazać należy, że obowiązek zgłaszania przez administratorów naruszeń ochrony danych osobowych Prezesowi UODO, w tym deklarowanie konkretnych działań i rozwiązań, jakie zastosowali lub zamierzają wdrożyć, by zapobiec podobnym naruszeniom w przyszłości, należy ocenić pozytywnie. Realizacja tych działań, która jest przez organ nadzorczy monitorowana, bez wątpienia przyczynia się do podniesienia poziomu ochrony danych osobowych.

8.2. Sektor prywatny

Zgłoszenia naruszeń ochrony danych osobowych z sektora prywatnego

W analizowanym roku sprawozdawczym do UODO wpłynęło **3303 zgłoszenia naruszeń** ochrony danych osobowych – głównie z sektora bankowego/ubezpieczeniowego i finansowego oraz firm telekomunikacyjnych. Zgłaszane naruszenia w większości przypadków posiadały charakter drobnych incydentów, na ogół dotyczących przetwarzania danych osobowych jednej lub kilku osób, spowodowanych błędem ludzkim np. przypadki przesłania danych osobowych do niewłaściwego odbiorcy, na niewłaściwy adres poczty elektronicznej/adres do korespondencji, omyłkowego wysyłania dokumentacji do innego odbiorcy oraz zagubienia przez pracowników dokumentów zawierających dane osobowe klientów (dotyczy to głównie pracowników, których praca polega na kontaktach z klientem w miejscu jego zamieszkania, np. agentów ubezpieczeniowych).

Ale wśród odnotowanych zgłoszeń były także liczne przypadki naruszeń polegających na kradzieży baz danych przez pracowników firm, a potem sprzedawanie na internetowych portalach aukcyjnych. Tendencję wzrostową posiadały również zgłoszenia naruszeń ochrony danych osobowych polegające na zagubieniu dokumentacji w formie papierowej przez operatorów pocztowych oraz podmioty świadczące usługi kurierskie. W przypadkach **naruszeń ochrony danych osobowych spowodowanych zaginięciem lub nieprawidłowym doręczeniem przesyłek pocztowych,** Prezes UODO wskazywał, że to nadawca powinien każdorazowo informować organ

nadzorczy o tego rodzaju naruszeniach, jako administrator danych osobowych przetwarzanych w związku z realizacją swoich zadań.

Prezes UODO nie przyjmował w tym zakresie argumentacji niektórych nadawców masowych, zgodnie z którą to operator pocztowy powinien przekazać wyjaśnienie w zakresie naruszenia organowi nadzorczemu oraz to on powinien zawiadomić o naruszeniu osobę, której dane dotyczą. Tylko nadawca bowiem posiada wiedzę o tym, jakie dane przekazywane są w przesyłce, a tym samym może ocenić, jakim ryzykiem dla praw i wolności osoby fizycznej skutkuje utrata przesyłki, i ma tym samym możliwość wykonania obowiązku z art. 33 i 34 RODO. Operator pocztowy w przedmiotowej sprawie takiej wiedzy nie posiada i posiadać nie może. Zgodnie z art. 41 ust. 1 ustawy Prawo Pocztowe, operatorzy pocztowi zobowiązani są do ochrony tajemnicy pocztowej obejmującej informacje przekazywane w przesyłkach pocztowych. Mają oni obowiązek zachowania należytej staranności w zakresie uzasadnionym względami technicznymi lub ekonomicznymi przy zabezpieczaniu urządzeń i obiektów wykorzystywanych przy świadczeniu usług pocztowych oraz zbiorów danych przed ujawnieniem tajemnicy pocztowej (art. 41 ust. 6 ustawy Prawo pocztowe). W momencie przyjęcia przesyłki operator pocztowy ma obowiązek wykonać usługę z należytą starannością i w tym zakresie podlega odpowiedzialności wynikającej z rozdziału 8 ustawy Prawo pocztowe. Podmioty korzystające z usług operatorów pocztowych mają zatem w tym zakresie do dyspozycji określone przepisami prawa środki egzekwowania należytego wykonania umowy o świadczenie usług pocztowych.

Administratorzy próbują zabezpieczać się na takie ewentualności i w wielu przypadkach kwestie związane z niezrealizowaniem przesyłek są uregulowane w indywidualnych umowach pomiędzy nimi a operatorami pocztowymi – tu często mają zastosowanie kary umowne. Mimo to problem z zagubionymi przesyłkami, w których są dane osobowe, ma miejsce i jest bardzo dotkliwy dla administratorów i osób, których dane dotyczą. Dlatego w 2019 r. Prezes UODO wspólnie z Urzędem Komunikacji Elektronicznej sygnalizował rynkowi pocztowemu, że powinny zostać wypracowane działania, które by ten problem ograniczyły. Wskazywał przy tym, że operatorzy również odpowiadają za bezpieczeństwo tych przesyłek i należyte wykonywanie usług. Obowiązuje ich także tajemnica pocztowa, o której mówi art. 42 ustawy – Prawo pocztowe. Przypomniał także administratorom o ich obowiązkach m.in. w zakresie zabezpieczenia danych i zachęcał, by administratorzy, którzy korzystają z usług pocztowych wspólnie z operatorami wypracowali zasady współpracy na wypadek zagubienia korespondencji. Takie mechanizmy powinny umożliwiać sprawną obustronną komunikację między tymi podmiotami, aby jak najszybciej zapewniać odpowiednią ochronę utraconym danym lub podjąć działania minimalizujące negatywne

konsekwencje takich naruszeń. Chodzi tu np. o szybkie sygnalizowanie problemów z dostarczeniem przesyłek, czy usprawnienie postępowań reklamacyjnych, a także prace nad rozwiązaniami zmierzającymi do wyeliminowania nieprawidłowości polegających na gubieniu przesyłek lub ich dostarczaniu pod niewłaściwy adres. Prezes UODO zachęcał również, by organizacje zrzeszające operatorów pocztowych tworzyły kodeksy postępowań, w których uregulowane zostałyby zasady postępowania na wypadek zgubienia przesyłki oraz mechanizmy powiadamiania o tym nadawcy. Praca nad kodeksami może być też doskonałą okazją do tego, by przejrzeć dotychczasowe procedury i rozwiązania w celu ich ewentualnej modyfikacji pod kątem ograniczenia ryzyka zgubienia przesyłek z danymi osobowymi lub dostarczania takiej korespondencji pod inny adres.

W wielu przypadkach zagubionej przesyłki nie udało się odnaleźć.

Najczęściej zgłaszane w 2019 r. naruszenia ochrony danych osobowych przez administratorów sektora prywatnego można pogrupować według następujących zagadnień:

1. *Udostępnienie danych osobie innej niż adresat – nieprawidłowo zaadresowana korespondencja (w formie tradycyjnej oraz za pomocą poczty elektronicznej).* Naruszenia o charakterze incydentalnym, wynikające z błędów pracowników. W ramach działań minimalizujących ryzyko ponownego wystąpienia naruszenia administratorzy przeprowadzali dodatkowe szkolenia, audyty bezpieczeństwa, dyscyplinowali pracowników, dokonywali przeglądu wdrożonych procedur oraz zobowiązywali osoby nieuprawnione, które weszły w posiadanie tych dokumentów, do ich zwrotu.
2. *Wysyłka poczty elektronicznej do wielu adresatów z pominięciem aktywnej opcji „Ukryj do wiadomości"*, naruszenia wynikające z błędu ludzkiego, najczęściej w momencie dokonywania przez pracowników seryjnej wysyłki korespondencji. W ramach działań minimalizujących ryzyko ponownego wystąpienia naruszenia, administratorzy przeprowadzali szkolenia pracowników z zakresu korzystania z poczty elektronicznej oraz dokonywali przeglądu wdrożonych procedur.
3. *Błędy programistyczne w systemach informatycznych pozwalające na uzyskanie dostępu do danych osobowych przez osoby do tego nieuprawnione.* Najczęstszą przyczyną tego typu naruszeń były błędy ujawniające się po wprowadzeniu aktualizacji danego oprogramowania lub brak wewnętrznych testów bezpieczeństwa, które mogły wykazać podatności systemu. W ramach działań minimalizujących ryzyko ponownego wystąpienia naruszenia, administratorzy decydowali o wcześniejszym dokładniejszym testowaniu oprogramowania/systemu w środowisku deweloperskim.

4. *Ataki hakerskie skutkujące uzyskaniem nieuprawnionego dostępu do bazy danych.* Naruszenia wynikały z podatności atakowanych systemów oraz wyspecjalizowanych umiejętności osób przeprowadzających tego typu ataki. Administratorzy w ramach działań naprawczych dokonywali przeglądu wdrożonych zabezpieczeń oraz zlecali wykonywanie testów bezpieczeństwa podmiotom wyspecjalizowanym w danej dziedzinie, co umożliwiało znaczne podniesienie stopnia stosowanych zabezpieczeń. Powiadamiano również organy ścigania.

5. *Zagubienie dokumentacji zawierających dane osobowe,* głównie w formie papierowej przez operatorów pocztowych lub podmioty świadczące usługi kurierskie. W ramach działań naprawczych administratorzy dokonywali przeglądu umów zawartych z tymi podmiotami oraz ustalano przyczyny zaistniałych zdarzeń.

6. *Udostępnienie danych w formie papierowej lub elektronicznej osobie nieuprawnionej.* W tym przypadku do naruszeń dochodziło w skutek omyłkowo zaksięgowanych przelewów, wydawania dokumentów (np. formularzy) zawierających dane osobowe innych osób. Administratorzy podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia, dokonywali przeglądu procedur, oraz zobowiązywali osoby nieuprawnione, które weszły w posiadanie tych dokumentów do ich zwrotu.

7. *Publikacja danych osobowych na stronie internetowej administratora* – w ramach działań naprawczych administratorzy usuwali treści ze swoich witryn internetowych.

8. *Kradzież baz danych klientów przez pracowników.* Tego typu naruszenia występują na coraz większą skalę w sektorze bankowym oraz ubezpieczeniowym. Pracownicy w momencie ustania stosunku pracy przenosili potencjalną bazę danych klientów do nowego pracodawcy (np. banku), która następnie była przez nich ponownie wykorzystywana. Dane osobowe wykradzione w ten sposób były również oferowane na internetowych portalach aukcyjnych. W przypadku zaistnienia tego typu naruszeń powiadamiane były organy ścigania. Minimalizując ryzyko ponownego wystąpienia naruszenia podmioty wdrażają m.in. systemy DLP (Data Loss Prevention), które posiadają zdefiniowane reguły m.in. w zakresie przesyłania plików przez pocztę elektroniczną do adresatów zewnętrznych; wgrywanie plików na stronach internetowych; nagrywane plików na nośniki USB oraz przesyłanie danych na prywatne skrzynki pocztowe pracowników.

W **dwóch przypadkach** wynikających ze zgłoszonych naruszeń ochrony danych osobowych, Prezes UODO nałożył administracyjne kary pieniężne (Dolnośląski Związek Piłki Nożnej oraz Morele.Net Sp. z o.o.).

W celu wyeliminowania nieprawidłowości dotyczących zgłoszeń naruszeń ochrony danych osobowych i udzielenia wskazówek, UODO podjął następujące działania:

a) **wykonał 900 rozmów telefonicznych oraz wysłał 250 e-maili do administratorów i inspektorów ochrony danych** – taka forma kontaktu z administratorami i inspektorami ochrony danych uzasadniona jest z uwagi na konieczność podejmowania szybkich działań mających na celu ochronę praw lub wolności osób fizycznych;

b) **skierował do administratorów ok. 630 wezwań dotyczących złożenia wyjaśnień w zakresie nadesłanych zgłoszeń naruszeń** – wezwania dotyczyły m.in. sytuacji, gdy przesłane zgłoszenia były niepełne lub niejasne, a kontakt z IOD lub innym punktem kontaktowym był utrudniony;

c) **skierował do administratorów ok. 700 wystąpień z żądaniem zawiadomienia osoby/osób, której/których dane dotyczą, w sytuacji, gdy zawiadomienie takie nie nastąpiło, a w ocenie UODO było ono uzasadnione; lub ponownego zawiadomienia, jeżeli zawiadomienie nie spełniało wymogów określonych w art. 34 RODO.** W wystąpieniach Prezes UODO dodatkowo przekazywał wskazówki dotyczące prawidłowego zawiadomienia osób, których dane dotyczą o naruszeniu oraz wzywał administratora do przekazania UODO informacji, jakie działania zostały podjęte;

d) **skierował do administratorów 43 decyzje administracyjne nakazujące zawiadomienie lub ponowne prawidłowe zawiadomienie osób**, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. Postępowania administracyjne w sprawach naruszeń wszczynane były w sytuacji, gdy administrator nie zawiadomił osoby, której dane dotyczą, o naruszeniu, a jest to uzasadnione z uwagi na występowanie wysokiego ryzyka dla praw i wolności tej osoby.

8.3. Działalność informacyjno-edukacyjna w sprawach naruszeń

Po roku stosowania RODO, na stronie internetowej UODO opublikowane zostały obszerne wskazówki dotyczące naruszeń ochrony danych pod tytułem „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych”[177] wraz ze statystykami dotyczącymi zgłoszeń z okresu 25 maja 2018 r. do 25 maja 2019 r. – pierwszego roku stosowania przepisów RODO. W poradniku tym znalazły się między innymi wskazówki dotyczące pojęcia naruszenia ochrony danych osobowych, kiedy i w jaki sposób trzeba powiadomić Prezesa UODO o naruszeniu, jakie są najczęściej popełniane błędy podczas zgłaszania naruszeń oraz w jaki sposób należy oceniać ryzyko

[177] https://uodo.gov.pl/pl/134/1029

naruszenia praw lub wolności osób fizycznych na wypadek stwierdzenia naruszenia. W poradniku znalazły się również podpowiedzi dotyczące prawidłowego zawiadomienia osób, których dane dotyczą o naruszeniu, a także informacje na temat obowiązków administratorów związanych z naruszeniami wynikających z innych niż rozporządzenie ogólne o ochronie danych, przepisów prawa (ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, rozporządzenie eIDAS – Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, ustawy z dnia 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa).

Wsparciem dla administratorów są także porady telefoniczne w związku z uruchomieniem dodatkowej infolinii dedykowanej dla IOD, na bieżąco aktualizowane na stronie internetowej UODO informacje w zakładce „Administrator”[178] dotyczące obowiązków administratorów w związku z naruszeniami ochrony danych osobowych oraz w zakładce „Inspektor Ochrony Danych”[179], a także wydawanie newslettera dla IOD[180]. W 2019 roku przeprowadzono również liczne szkolenia oraz konferencje, na których omawiano zagadnienia związane z problematyką naruszeń, zamieszczono liczne materiały na stronie internetowej oraz podniesiono poziom komunikacji z administratorami danych.

9. Administracyjne kary pieniężne

W toku przeprowadzonych postępowań w **8 przypadkach** Prezes Urzędu Ochrony Danych Osobowych, stosując przysługujące mu rozwiązania naprawcze przewidziane w art. 58 ust. 2 RODO, zdecydował o nałożeniu kary administracyjnej. Karą objęte zostały następujące podmioty: spółka prowadząca sprzedaż online, spółka przetwarzająca dane z rejestrów publicznych, wspólnota mieszkaniowa, spółka zajmująca się ochroną mienia i ludzi, stowarzyszenie sportowe, spółka zarządzająca nieruchomościami, burmistrz miasta oraz spółka prowadząca marketing w sieci. Nakładając kary organ nadzorczy podkreślił, że stwierdzone naruszenia miały znaczną wagę oraz poważny charakter.

[178] https://uodo.gov.pl/pl/p/najwazniejsze-tematy/administrator
[179] https://uodo.gov.pl/pl/p/najwazniejsze-tematy/administrator
[180] Dostępny pod adresem: https://news.uodo.gov.pl/lists/. Teraz Inspektorzy Ochrony Danych Osobowych mają zapewniony stały dostęp do specjalistycznej wiedzy o ochronie danych osobowych oraz przydatnych i najbardziej aktualnych informacji dotyczących tej problematyki. Newsletter dla IOD przyczynił się do usprawnienia elektronicznej formy kontaktu IOD z Urzędem Ochrony Danych Osobowych.

Poniżej przedstawione zostały wybrane przykłady decyzji Prezesa UODO w oparciu o art. 83 RODO, które zakończyły się nałożeniem administracyjnej kary pieniężnej.

- Kara pieniężna w wysokości 55 750,50 PLN nałożona na **Dolnośląski Związek Piłki Nożnej** z siedzibą we Wrocławiu[181] była skutkiem stwierdzenia naruszenia ochrony danych osobowych polegającego na niezapewnieniu bezpieczeństwa i poufności przetwarzanych danych 585 osób, którym przyznano licencje sędziowskie w roku 2015, poprzez ich nieuprawnione ujawnienie na stronie internetowej Dolnośląskiego Związku Piłki Nożnej. Dane osobowe upublicznione w sieci obejmowały nie tylko imiona i nazwiska sędziów, ale także ich adresy zamieszkania oraz numery PESEL. Prezes Urzędu Ochrony Danych Osobowych uwzględnił też okoliczności łagodzące, którymi były m.in. brak dowodów na to, że powstały szkody po stronie osób, których dane ujawniono. Decyzja Prezesa UODO została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie[182].
- Kara pieniężna w wysokości 2 830 410 PLN została nałożona na **Morele.Net Sp. z o.o.** z siedzibą w Krakowie[183], za dwa naruszenia ochrony danych osobowych. W wyniku uzyskania przez osobę nieuprawnioną dostępu do bazy danych klientów realizujących zakupy w sklepach internetowych, dane ponad 2 milionów osób (użytkowników sklepów internetowych, których Morele.Net. jest administratorem) dostały się w niepowołane ręce. W toku przeprowadzonych czynności kontrolnych ustalono, że do naruszenia doszło z uwagi na nieskuteczne monitorowanie potencjalnych zagrożeń. Postępowanie wykazało także uchybienia w postaci braku odpowiednich środków technicznych (niewystarczające zabezpieczenia) i organizacyjnych (dotyczących monitorowania potencjalnych zagrożeń, związanych z nietypowymi zachowaniami w sieci), które ostatecznie przesądziły o nałożeniu kary. W decyzji nakładającej karę organ nadzorczy uznał, że spółka nie stosując wystarczających środków technicznych ochrony danych naruszyła m.in. określoną w art. 5 ust. 1 lit. f RODO zasadę poufności. Organ uznał, że miało też miejsce zastosowanie nieskutecznego środka uwierzytelniania dostępu do danych. Dodatkowe środki zabezpieczenia technicznego spółka wdrożyła już po naruszeniu. Celem nałożonej kary było doprowadzenie do właściwego wykonywania przez spółkę obowiązków przewidzianych w art. 5 ust. 1 lit. f, art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 lit. b i d, art. 32 ust. 2 RODO, a w konsekwencji do prowadzenia procesów przetwarzania danych zgodnie z obowiązującymi

[181] ZSPR.440.43.2019
[182] Wyrokiem z 28 lutego 2020 r. WSA w Warszawie utrzymał w mocy decyzję Prezesa UODO nakładającą administracyjną karę pieniężną na Dolnośląski Związek Piłki Nożnej, zob. także https://uodo.gov.pl/pl/138/1448.
[183] ZSPR.421.2.2019

przepisami prawa. Wydając decyzję organ nadzorczy stwierdził, że naruszenie, do jakiego doszło w tej sprawie, miało znaczną wagę, poważny charakter i dotyczyło dużej liczby osób, w skutek czego powstało wysokie ryzyko negatywnych skutków dla osób, których dane zostały udostępnione osobom nieuprawnionym. Decyzja Prezesa UODO została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie.

- Pierwsza kara pieniężna za niedopełnienie obowiązku informacyjnego wobec osób prowadzących działalność gospodarczą została nałożona przez Prezesa Urzędu Ochrony Danych Osobowych na **Bisnode Polska Sp. z o.o.** Decyzja Prezesa UODO[184] dotyczyła postępowania związanego z działalnością spółki, która przetwarza dane osób pozyskane ze źródeł publicznie dostępnych, m.in. z Centralnej Ewidencji i Informacji Działalności Gospodarczej (CEiDG) w celach zarobkowych. Organ nadzorczy weryfikował niedopełnienie obowiązku informacyjnego wobec osób fizycznych prowadzących działalność gospodarczą – przedsiębiorców, którzy aktualnie ją prowadzą, bądź tę działalność zawiesili, jak i tych, którzy prowadzili ją w przeszłości. Obowiązek informacyjny, o którym mowa w art. 14 RODO, został przez Bisnode Polska dopełniony wyłącznie w odniesieniu do 682439 osób fizycznych prowadzących działalność gospodarczą, których dane osobowe podmiot ten przetwarza w systemie informatycznym. Natomiast obowiązek nie został przez spółkę spełniony w stosunku do pozostałych osób fizycznych prowadzących działalność gospodarczą, które nie posiadały adresu e-mail w bazie danych, przy czym zarówno chodzi o przedsiębiorców, którzy prowadzą aktualnie działalność gospodarczą, jak i o tych, którzy zaprzestali jej prowadzenia. W przypadku pozostałych osób spółka tego obowiązku nie dopełniła – jak sama to wyjaśniła w toku postępowania – z uwagi na wysokie koszty takiej operacji. Dlatego jedynie na swojej stronie internetowej zamieściła klauzulę informacyjną.

Prezes Urzędu Ochrony Danych Osobowych stwierdził, że samo umieszczenie informacji, wymaganych w art. 14 ust. 1 i ust. 2 RODO, na stronie internetowej spółki, w sytuacji posiadania przez Bisnode Polska danych adresowych osób fizycznych prowadzących jednoosobową działalność gospodarczą, umożliwiających przesłanie pocztą tradycyjną korespondencji zawierającej wymagane tym przepisem informacje (lub przekazanie ich drogą kontaktu telefonicznego), nie może być uznane za wystarczające spełnienie obowiązku, o którym mowa w art. 14 ust. 1-3 RODO. Mając dane kontaktowe do poszczególnych osób, administrator ten powinien spełnić wobec osób obowiązek informacyjny, podając im stosowne informacje. W ocenie Prezesa UODO wysłanie informacji, o których mowa w art. 14 RODO, pocztą tradycyjną, na adres

[184] ZSPR.421.3.2019

osoby fizycznej prowadzącej działalność gospodarczą, lub w drodze kontaktu telefonicznego, nie jest czynnością „niemożliwą" oraz nie wymaga „niewspółmiernie dużego wysiłku", w sytuacji posiadania przez spółkę w bazie systemu informatycznego danych adresowych, w odniesieniu do osób fizycznych prowadzących jednoosobową działalność gospodarczą, a także dodatkowo – numerów telefonów – w odniesieniu do części tych osób. Prezes UODO uznał, że naruszenie administratora miało charakter umyślny, ponieważ – jak ustalono w toku postępowania – spółka miała świadomość istnienia obowiązku podania stosownych informacji, jak i konieczności bezpośredniego informowania osób. Wymierzając karę, organ wziął pod uwagę również fakt, że administrator nie podjął żadnych działań zmierzających do usunięcia naruszenia ani nie zadeklarował takiego zamiaru.

Decyzja ta miała i ma wpływ na bardzo dużą ilość osób, wobec których obowiązek informacyjny nie został spełniony. Znaczenie mają też konsekwencje niespełniania tego obowiązku jakimi są: niewiedza osób, których dane dotyczą o procesach przetwarzania ich danych oraz o możliwości skorzystania z przysługujących im praw zagwarantowanych przepisami RODO. Także czas trwania naruszenia ocenić należy negatywnie, mając na uwadze termin wejścia w życie RODO i termin rozpoczęcia jego stosowania. Znaczenie w tej sprawie ma także to, że naruszenie dotyczy – zgodnie z art. 83 ust. 5 lit b RODO – jednego z podstawowych praw osób, do którego zastosowanie ma wyższa kwota administracyjnej kary pieniężnej[185].

Prezes Urzędu Ochrony Danych Osobowych, korzystając z przysługującego mu uprawnienia określonego w art. 58 ust. 2 lit. d RODO, nakazał spółce w terminie do trzech miesięcy od daty otrzymania decyzji, dopełnienie obowiązku podania informacji, o których mowa w art. 14 ust. 1 i 2 RODO, tym osobom fizycznym prowadzącym aktualnie lub w przeszłości jednoosobową działalność gospodarczą, których dane osobowe przetwarza, a którym informacje te nie zostały podane. W ocenie Prezesa UODO zastosowana kara pieniężna (w wysokości ponad 943 tys. zł) spełnia w ustalonych okolicznościach tej sprawy przesłanki, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679 ze względu na powagę stwierdzonych naruszeń w kontekście podstawowych wymogów i zasad rozporządzenia 2016/679 – rzetelności i przejrzystości oraz prawa do informacji.

[185] Ww. przepis stanowi, że naruszenia przepisów dotyczących praw osób, których dane dotyczą (w tym prawa do uzyskania informacji, o których mowa w art. 14 ust. 1 i 2 tego rozporządzenia), podlegają administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Decyzja Prezesa UODO została zaskarżona przez spółkę do Wojewódzkiego Sądu Administracyjnego w Warszawie[186].

- Prezes Urzędu Ochrony Danych Osobowych nałożył karę pieniężną na **ClickQuickNow Sp. z o.o**. w wysokości ponad 201 tys. zł m.in. za utrudnianie realizacji prawa do wycofania zgody na przetwarzanie danych osobowych[187]. Ukarana przez Prezesa UODO spółka nie wdrożyła odpowiednich środków technicznych i organizacyjnych, które umożliwiałyby łatwe i skuteczne wycofanie zgody na przetwarzanie danych osobowych oraz realizację prawa do żądania usunięcia danych osobowych (prawa do bycia zapomnianym). Naruszyła więc określone w RODO zasady zgodności z prawem, rzetelności i przejrzystości przetwarzania danych osobowych.

Prezes UODO w decyzji uznał, że działanie spółki było niezgodne z art. 7 ust. 3 RODO. Spółka w procesie wycofania zgody nie uwzględniła zasady, zgodnie z którą wycofanie zgody powinno być równie łatwe jak jej wyrażenie. Wręcz odwrotnie – spółka stosowała dla wycofania zgody skomplikowane rozwiązania organizacyjne i techniczne. Ponadto spółka nie ułatwiała realizacji praw osobom, których dane przetwarzała, a wymaga tego art. 12 ust. 2 RODO. Postępowanie Prezesa UODO wykazało, że podmiot ten naruszył powyższe przepisy RODO, gdyż stosowany przez niego mechanizm wycofywania zgody, polegający na użyciu linku zamieszczonego w treści informacji handlowej, nie skutkował szybkim wycofaniem zgody. Po uruchomieniu linku, komunikaty kierowane do osoby zainteresowanej wycofaniem zgody wprowadzały ją w błąd. Ponadto spółka bezprawnie wymuszała podanie przyczyny wycofania zgody, a brak wskazania przyczyny skutkował przerwaniem procesu wycofania zgody. Co więcej, spółka przetwarzała bez podstawy prawnej dane osób, które nie są jej klientami, a od których otrzymała żądania zaprzestania przetwarzania ich danych osobowych. Naruszyła więc także przepisy dotyczące tzw. prawa do usunięcia danych – „prawa do bycia zapomnianym''. Ustalając wysokość administracyjnej kary pieniężnej, Prezes Urzędu Ochrony Danych Osobowych nie uwzględnił żadnej okoliczności łagodzącej mającej wpływ na ostateczny wymiar kary. Uznał też, że działanie spółki było umyślne, gdyż przekazywanie osobie zainteresowanej wycofaniem zgody sprzecznych ze sobą komunikatów skutkowało tym, że wycofanie zgody nie było skuteczne. W ten sposób spółka utrudniała, a wręcz uniemożliwiała realizację praw osób, których dane dotyczą. Prezes UODO nie tylko nałożył karę finansową na ClickQuickNow, ale nakazał jej także

[186] W dniu 11 grudnia 2019 r. przed WSA w Warszawie zapadł wyrok w tej sprawie (sygn. II SA/Wa 1030/19).
[187] ZSPR.421.7.2019

dostosowanie do przepisów RODO procesu obsługi wniosków o wycofanie zgody na przetwarzanie danych.

Decyzja Prezesa UODO została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie.

W analizowanym 2019 r. Prezes UODO nałożył także **4 administracyjne kary pieniężne na podmioty sektora publicznego**[188].

Szczególnie istotna, z punktu widzenia poprawnego kształtowania zasad przetwarzania danych osobowych przez jednostki samorządu terytorialnego, była kara w wysokości 40 tys. zł nałożona na **burmistrza miasta Aleksandrów Kujawski**, który ani z firmą, na której serwerach znalazły się zasoby Biuletynu Informacji Publicznej (BIP) Urzędu Miejskiego, ani z firmą, która dostarczała oprogramowanie do stworzenia BIP i zajmowała się obsługą serwisową w tym zakresie, nie zawarł umowy powierzenia przetwarzania danych osobowych.

Prezes UODO uznał więc, że doszło do naruszenia art. 28 ust. 3 RODO. Przepis ten zobowiązuje administratora, w imieniu którego przetwarzania danych osobowych dokonuje inny podmiot, do zawarcia z nim umowy powierzenia. W konsekwencji braku takiej umowy burmistrz dopuścił się udostępnienia danych osobowych bez podstawy prawnej, czym naruszył określone w RODO: zasadę przetwarzania danych zgodnie z prawem (art. 5 ust. 1 lit. a) oraz zasadę poufności (art. 5 ust. 1 lit. f). To jednak nie jedyne naruszenia, jakie stwierdzono w toku postępowania kontrolnego przeprowadzonego w tym podmiocie. Ustalono także, że brak było procedur wewnętrznych dotyczących przeglądu zasobów dostępnych w BIP pod kątem ustalenia okresu ich publikowania. To spowodowało, że przykładowo w BIP były dostępne m.in. oświadczenia majątkowe z 2010 roku, podczas gdy okres ich przechowywania wynosi 6 lat, co wynika z przepisów sektorowych. W przypadku danych, których okresu przechowywania nie reguluje prawo, administrator powinien sam go ustalić adekwatnie do celów, w jakich je przetwarza. Administrator naruszył więc zasadę ograniczonego przechowywania, określoną w art. 5 ust. 1 lit. e RODO.

W czasie postępowania ustalono również, że zarejestrowane materiały z posiedzeń rady miejskiej były dostępne w BIP jedynie poprzez zamieszczenie linku do dedykowanego kanału na YouTube. W Urzędzie Miejskim nie było kopii zapasowych tych nagrań. Przez to w przypadku utraty danych zapisanych w serwisie YouTube administrator nie dysponowałby tymi nagraniami. Nie przeprowadzono również analizy ryzyka związanego z publikacją nagrań z posiedzeń rady

[188] ZSPU.421.3.2019, ZSPU.421.13.2019, ZSPU.421.14.2019, ZSPU.421.16.2019.

wyłącznie w serwisie YouTube. Doszło więc do naruszenia zasady integralności i poufności (art. 5 ust. 1 lit. f) oraz zasady rozliczalności (art. 5 ust. 2).

Zasada rozliczalności została naruszona również w związku z brakami w rejestrze czynności przetwarzania. Nie było w nim np. wskazanych wszystkich odbiorców danych, a także brakowało wskazania planowanego terminu usunięcia danych dla niektórych czynności przetwarzania. Prezes UODO, nakładając karę, wziął pod uwagę to, że mimo stwierdzonych w toku postępowania nieprawidłowości, nie zostały one usunięte przez administratora, ani nie wdrożył on rozwiązań mających przeciwdziałać naruszeniom w przyszłości. Administrator nie współpracował również z organem nadzoru. Dlatego Prezes UODO uznał, że nie zachodziły przesłanki, które mogłyby złagodzić wysokość kary. Oprócz kary pieniężnej Prezes Urzędu nakazał również administratorowi podjęcie działań mających na celu usunięcie stwierdzonych naruszeń w ciągu 60 dni.

W 2019 r. administracyjne kary pieniężne zostały nałożone także na wspólnotę mieszkaniową (2 tys. zł), spółkę zarządzającą nieruchomościami (8 tys. zł) oraz spółkę zajmującą się ochroną osób i mienia (30 tys. zł). W podmiotach tych stwierdzono bowiem uchybienia związane z przetwarzaniem danych w ramach monitoringu wizyjnego.

W odniesieniu do **spółki zarządzającej nieruchomościami** ustalono, że w procesie przetwarzania danych w ramach monitoringu wizyjnego stosowanego w jednej z warszawskich nieruchomości, doszło do uchybień, które polegały na: przetwarzaniu danych pochodzących z monitoringu wizyjnego bez umowy powierzenia przetwarzania danych (co stanowiło naruszenie art. 5 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych) oraz niewdrożeniu przez ww. podmiot środków organizacyjnych i technicznych w związku ze stosowaniem monitoringu wizyjnego, zapewniających kontrolę nad udostępnianymi danymi osobowymi z monitoringu wspólnoty mieszkaniowej (naruszono w ten sposób art. 5 ust. 1 lit. f RODO).

Z kolei **spółka zajmująca się ochroną osób i mienia**, działając jako podmiot przetwarzający, w związku z nienadaniem upoważnień do przetwarzania danych osobowych każdemu pracownikowi ochrony mającemu dostęp do monitoringu wizyjnego, nie zapewniła prawidłowej kontroli nad procesem przetwarzania danych osobowych zebranych w związku z funkcjonującym we wspólnocie mieszkaniowej monitoringiem wizyjnym, a tym samym naruszyła przepisy art. 28 i art. 29 ogólnego rozporządzenia o ochronie danych.

Natomiast uchybienia stwierdzone we **wspólnocie mieszkaniowej**, będącej administratorem, polegały na naruszeniu:

- art. 5 ust. 2 w związku z art. 5 ust. 1 lit. f i art. 24 ust. 1 RODO, tj. zasady rozliczalności oraz zasady integralności i poufności, poprzez niewdrożenie narzędzi umożliwiających rozliczalność w zakresie udostępniania nagrań z monitoringu, w szczególności brak procedur dotyczących zarządzania systemem monitoringu, m.in. w zakresie udostępniania nagrań z monitoringu oraz ewidencjonowania dokonanych udostępnień;
- art. 5 ust. 1 lit. f RODO, tj. zasady integralności i poufności poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających odpowiednie bezpieczeństwo danych osobowych przetwarzanych za pomocą monitoringu wizyjnego, w tym ich ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;
- art. 5 ust. 1 lit. a w związku z art. 12 ust. 1 oraz art. 13 ust. 1 i 2 RODO, tj. zasady przejrzystości w związku z niespełnieniem obowiązku informacyjnego w sposób przejrzysty dla osoby, której dane dotyczą, w związku z przetwarzaniem danych pochodzących ze stosowanego monitoringu wizyjnego;
- art. 28 ust. 3 i ust. 9 oraz art. 5 ust. 1 lit. f RODO, tj. zasady integralności i poufności w związku z brakiem umowy powierzenia przetwarzania danych osobowych pochodzących z monitoringu wizyjnego.

10. Uprzednie konsultacje

Do zadań Urzędu Ochrony Danych Osobowych należy 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 niewielkim zakresie korzystali z tej formy współpracy z organem nadzorczym. W 2019 r. do Urzędu wpłynęło **5 wniosków**

o przeprowadzenie uprzednich konsultacji. Wnioski te dotyczyły zarówno planowanych procesów przetwarzania danych osobowych, jak i już realizowanych procesów przetwarzania.

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.

11. Kodeksy postępowania

Na mocy art. 40 RODO, wprowadzony został instrument prawny w postaci kodeksów postępowań, których celem jest pomoc we właściwym stosowaniu nowych przepisów o ochronie danych osobowych. Kodeksy postępowania są sporządzane przez zrzeszenia i inne podmioty, reprezentujące określone kategorie administratorów lub podmioty przetwarzające, które przedkładają projekt kodeksu organowi nadzorczemu. Następnie organ wydaje opinię o zgodności projektu kodeksu z RODO i jeżeli uzna, że zawiera on odpowiednie zabezpieczenie dla ochrony danych – zatwierdza go. W kolejnym etapie organ rejestruje i publikuje ten kodeks (o ile nie dotyczy on czynności przetwarzania prowadzonych w kilku państwach członkowskich). Stosowanie zatwierdzonego kodeksu postępowania stanowi okoliczność, na podstawie której będzie można stwierdzić, że podmiot wywiązuje się z ciążących na nim obowiązków, nałożonych przez przepisy o ochronie danych osobowych.

W 2019 r. w ramach realizacji zadania z art. 57 ust. 1 lit. m RODO, Prezes UODO najczęściej zachęcał do przygotowywania **kodeksów postępowania** określonych w art. 40 RODO, podczas szkoleń i spotkań z administratorami i inspektorami ochrony danych oraz w artykułach prasowych. W szczególności podczas szkoleń współorganizowanych z Narodowym Instytutem Samorządu Terytorialnego oraz VI Ogólnopolskiej Konferencji Samorządu i Oświaty Edukacja Przyszłości w Lublinie, przedstawiciele Urzędu zachęcali do podejmowania prac nad kodeksami dla sektora oświaty oraz administracji lokalnej.

Na stronie internetowej Urzędu utworzono **zakładkę dotyczącą kodeksów postępowania**[189], która zawiera m.in. wyjaśnienia przepisów regulujących to narzędzie zapewniania zgodności

[189] Zob. https://uodo.gov.pl/425

z prawem ochrony danych, informacje o aktualnych działaniach UODO (w tym wykaz złożonych wniosków o zatwierdzenie kodeksów wraz z ich projektami) oraz informacje o działaniach Europejskiej Rady Ochrony Danych (m.in. konsultacje projektów wytycznych Rady).

W 2019 r. odbyło się **20 indywidualnych spotkań z autorami kodeksów**, podczas których przedstawiciele Urzędu m.in. 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.

W 2019 r. złożono **1 wniosek o zatwierdzenie projektu kodeksu**. Był to „Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez spółdzielnie mieszkaniowe zrzeszone w Związku Rewizyjnym Spółdzielni Mieszkaniowych RP".

W toku prowadzonych postępowań pracownicy UODO spotykali się z autorami kodeksów celem omówienia poszczególnych postanowień, oceny sprawozdania z konsultacji i innych elementów wniosku. Dużym wyzwaniem dla podmiotów zrzeszonych było nadal przyjęcie modelu monitorowania kodeksu, który będzie akceptowalny dla członków z punktu widzenia działalności organizacji 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. Jednym z ich efektów było **skierowanie do Ministra Finansów wystąpienia o podjęcie inicjatywy ustawodawczej – zmiany Prawa bankowego,** poprzez rozszerzenie katalogu podmiotów, którym udzielane są informacje objęte tajemnicą bankową. Proponowane rozwiązanie umożliwi prowadzenie przez podmiot monitorujący efektywnego nadzoru przestrzegania **Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe,** którym objęta będzie działalność krajowych banków i rejestrów kredytowych zrzeszonych w Związku Banków Polskich.

Podsumowując, w 2019 r. odbyły się spotkania i opiniowanie kodeksów przedstawionych przez następujące podmioty:

- Związek Banków Polskich
- Stowarzyszenie Marketingu Bezpośredniego
- Polska Izba Przemysłowo-Handlowej Gospodarki Złomem
- IAB Polska (branża reklamy internetowej)
- Konferencja Przedsiębiorstw Finansowych
- OFBOR (podmioty prywatne zaangażowane w badania rynku i opinii, badania społeczne oraz analitykę danych – „Branża badawcza")

- PIIT (Polska Izba Informatyki i Telekomunikacji)
- Branża wodociągowo-kanalizacyjna
- Branża tłumaczy
- Stowarzyszenie Fotografów Komercyjnych

W omawianym roku 2019 rozpoczęte zostały też prace nad projektem **wymogów akredytacji podmiotu monitorującego**, które muszą zostać zaopiniowane przez Europejską Radę Ochrony Danych. W ramach **podgrupy Compliance, E-gov, Health Europejskiej Rady Ochrony Danych** przedstawiciele Prezesa Urzędu uczestniczyli w przygotowaniu Wytycznych 1/2019 w sprawie kodeksów postępowania i podmiotów monitorujących na mocy rozporządzenia 2016/679[190] i promowali informacje o konsultacjach publicznych tego dokumentu. Zatwierdzone wytyczne dostarczają 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. Przedstawiciele UODO uczestniczyli także w dyskusjach nad **projektami wymogów akredytacji podmiotu monitorującego** złożonych przez Austrię, Belgię, Czechy, Francję, Hiszpanię oraz Wielką Brytanię. Uzgodnione przez organy ochrony danych kryteria umożliwią rozpatrywanie wniosków o akredytację podmiotów monitorujących.

12. Pytania prawne i wystąpienia Prezesa UODO

Inicjowanie i podejmowanie działań w zakresie doskonalenia ochrony danych osobowych obejmuje w szczególności udzielanie odpowiedzi na pytania dotyczące interpretacji oraz stosowania przepisów prawa o ochronie danych osobowych, a także kierowanie wystąpień do właściwych podmiotów, w celu zapewnienia skutecznej ochrony danych osobowych. Mocą art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Prezes Urzędu może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych

[190] Zob. https://uodo.gov.pl/pl/138/732.

podmiotów, wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Podmiot, do którego skierowane zostało wystąpienie, obowiązany jest ustosunkować się do tego wystąpienia w terminie 30 dni od daty jego otrzymania.

12.1. Pytania prawne

Udzielanie odpowiedzi na pytania prawne dotyczące ochrony danych osobowych stanowi bardzo ważną – z punktu widzenia obywateli – działalność edukacyjną. Nie została ona ujęta w kompetencje organu właściwego w sprawach ochrony danych osobowych, niemniej jednak Prezes UODO docenia otrzymywane od obywateli sygnały dotyczące problemów związanych z interpretacją i stosowaniem przepisów prawa o ochronie danych osobowych. Treść kierowanych do UODO pytań prawnych stanowi często impuls do rozważenia podjęcia określonych działań z urzędu (np. wystąpienia, komunikaty na stronie internetowej organu, poradniki, wytyczne, itd.), których tematyka obejmuje niemalże wszystkie dziedziny życia publicznego.

W 2019 roku do Urzędu Ochrony Danych Osobowych wpłynęło łącznie **2812 pism zawierających pytania z zakresu ochrony danych osobowych.**

Zapytania dotyczące giełd długów.

Wiele wątpliwości osób kierujących pytania do Prezesa UODO budziła kwestia tzw. **giełd długów** w celu dokonania oceny, czy udostępnianie danych dłużników przez giełdy długów jest zgodne z rozporządzeniem 2016/679. Organ nadzorczy przedstawił stanowisko dotyczące przedmiotowej problematyki, które zostało zamieszczone w formie komunikatu na stronie internetowej UODO[191]. Wskazano, że przy dochodzeniu roszczeń jedną z przesłanek dopuszczalności przetwarzania danych osobowych, w tym ich udostępniania, jest realizacja prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (określoną w art. 6 ust. 1 lit. f RODO). Prawnie usprawiedliwionym celem może być m.in. dochodzenie roszczeń z tytułu prowadzonej przez administratora danych działalności gospodarczej. Przetwarzanie danych w takim przypadku jest prawnie dopuszczalne i nie odbywa się na podstawie zgody osoby, której dane dotyczą. Wskazano, że w ofercie sprzedaży wierzytelności można ujawnić dane osobowe dłużnika w zakresie jego imienia, nazwiska i adresu ze wskazaniem miasta, nazwy ulicy i kodu pocztowego, lecz bez numeru nieruchomości i numeru lokalu mieszkalnego. Zgodnie z zasadą „minimalizacji danych" wynikającą z RODO, udostępniane powinny być tylko te dane,

[191] https://uodo.gov.pl/pl/138/1263

które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do osiągnięcia celów przetwarzania. Podanie takich informacji o dłużniku jest uzasadnione, gdyż określa przeciwko komu wierzytelność przysługuje, ale jednocześnie nie stanowi zbytniej ingerencji w prywatność dłużnika. Wiedza o tym jest niezbędna dla racjonalnego podjęcia decyzji o nabyciu wierzytelności. Dlatego przedsiębiorca zajmujący się obrotem wierzytelnościami albo dochodzący swojej wierzytelności może, co do zasady, podawać do publicznej wiadomości niektóre dane osobowe dłużników w celu sprzedaży wierzytelności. Jego działanie należy uznać za legalne. Firma windykacyjna, która nabyła wierzytelność, staje się administratorem danych osobowych dłużników i zobowiązana jest do przestrzegania obowiązków wynikających z RODO. Powinna ona informować dłużników, wobec których prowadzone są działania windykacyjne, m.in. o podstawie prawnej i celu przetwarzania danych. Zasadniczo czyni to w pismach wzywających do zapłaty. Organ nadzorczy stoi na stanowisku, aby nie przekazywać danych przez telefon. Udostępnianie danych na odległość obarczone jest ryzykiem braku pewności co do tego, komu faktycznie dane są przekazane. Prawo do bycia zapomnianym nie ma zastosowania w przypadku dłużnika. Administrator, realizując wynikające z art. 17 RODO obowiązki, musi wziąć pod uwagę pewne ograniczenia wynikające z tej regulacji. W niektórych sytuacjach administrator wręcz nie może usunąć danych, np. gdy ich przetwarzanie wynika z realizacji ciążących na nim obowiązków prawnych. Powoływanie się bowiem na wynikające z RODO prawo do ochrony danych osobowych nie sprawi, że dłużnik uchyli się od spoczywającego na nim obowiązku spełnienia świadczenia, a wierzyciel nie będzie miał możliwości uzyskania należnej zapłaty.

Organ nadzorczy wskazał także, że możliwość przetwarzania danych osobowych przez komornika sądowego, podobnie jak w przypadku firm windykacyjnych, wynika również z przepisów, które dopuszczają możliwość przetwarzania danych osobowych dłużnika, jeżeli jest to niezbędne dla wypełnienia obowiązku wykonania czynności powierzonych ustawą. Dopuszczalność przetwarzania, w tym udostępniania danych osobowych przez komornika w określonej sytuacji, zależy od istnienia stosownej podstawy prawnej, od kategorii danych oraz od tego, jaki podmiot, na jakiej podstawie prawnej i w jakim celu wnioskuje o udostępnienie danych.

1% podatku na rzecz organizacji pożytku publicznego.

W związku z licznymi pytaniami od organizacji pożytku publicznego Prezes UODO zamieścił na stronie internetowej Urzędu komunikat dotyczący przetwarzania (w tym udostępniania danych osobowych) podatników (darczyńców) przekazujących 1 procent podatku na organizacje pożytku publicznego (OPP).

Dane podatnika, który w rozliczeniu rocznym PIT wyraził zgodę (jest ona dobrowolna) na przekazanie OPP swojego imienia, nazwiska i adresu, mogą być przetwarzane wyłącznie przez tę organizację. Jest to o tyle istotne, że w niektórych przypadkach środki z 1 proc. podatku trafiają do stowarzyszeń lub fundacji, które przekazują te środki do konkretnych osób, które wspierają. OPP może przetwarzać dane podatnika, np. w celu wysłania darczyńcy podziękowań w imieniu obdarowanego, o ile podatnik wyraził zgodę na przekazanie jego danych organizacji. Z chwilą, gdy OPP otrzymają od organów podatkowych dane osobowe darczyńców, staną się ich administratorami, czyli podmiotami decydującymi o celach i środkach przetwarzania tych danych. Będą zatem odpowiedzialne m.in. za właściwe ich wykorzystywanie, udostępnianie czy zabezpieczanie. Tym samym będą zobowiązane do przestrzegania przepisów ogólnego rozporządzenia o ochronie danych. Kierując korespondencję do darczyńców, OPP powinny zadbać, by został wobec nich spełniony obowiązek informacyjny, w tym poinformować o przysługujących tym osobom prawach. Organ nadzorczy wskazał, że organizacja pożytku publicznego nie ma jednak żadnych podstaw prawnych do udostępnienia danych darczyńców osobom obdarowanym, chyba że pozyskana byłaby na ten cel uprzednia zgoda. Warto więc o to zadbać planując tego typu działania. Dane osobowe darczyńców 1 proc. podatku przekazywane są organizacji pożytku publicznego przez naczelników urzędów skarbowych. Uprawnia ich do tego art. 45c ust. 5 ustawy o podatku dochodowym od osób fizycznych.

Legalność żądania od pracodawcy przez zakładową organizację związkową imiennej listy pracowników wraz z kwotą pobranych składek związkowych z ich wynagrodzenia.

W odpowiedzi na to pytanie skierowane do UODO przez jeden ze związków zawodowych, Prezes UODO wskazał, że podstawę pobierania z wynagrodzenia pracownika składki związkowej oraz przekazywania pobranych kwot na rachunek bankowy wskazany przez zakładową organizację związkową, stanowi art. 33^1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych[192]. Powyższy przepis wskazuje, że pracodawca za zgodą pracownika i na pisemny wniosek zakładowej organizacji związkowej, pobiera z wynagrodzenia pracownika składkę związkową. Prezes UODO odniósł się do art. 28 ustawy o związkach zawodowych, stanowiącego o pozyskiwaniu przez związki informacji od pracodawcy. W ust. 1 pkt 1 powyższego przepisu ustawodawca wskazał na informacje dotyczące warunków pracy i zasad wynagradzania. W ocenie Prezesa UODO informacja o zasadach wynagradzania nie daje podstawy prawnej do wnioskowania przez związki oraz

[192] Dz. U. z 2019 r. poz. 263 z późn. zm.

przekazywania przez pracodawcę informacji na temat wysokości wynagrodzenia poszczególnych pracowników. W opinii tej organ zaznaczył, że jeżeli przepisy prawa nie wskazują wprost na określone kompetencje związków zawodowych, to takiego uprawnienia nie można domniemywać. Wysokość wynagrodzenia to dane osobowe pracownika, które pracodawca ma obowiązek chronić przed nieuprawnionym dostępem. Obecnie w polskim systemie prawnym brak jest podstaw do tego, aby przekazywać związkom zawodowym imienny wykaz pracowników wraz z wysokością odprowadzanych przez nich składek, jeżeli wysokość potrącanej składki stanowiłaby informację o wysokości wynagrodzenia poszczególnych pracowników.

Prezes UODO wskazał, że należy rozróżnić sytuację, w której składka związkowa pobierana jest kwotowo, tj. w kwocie stałej dla wszystkich członków, oraz procentowo – od wysokości wynagrodzenia. Wyrażona przez pracowników zgoda na potrącanie z ich wynagrodzenia składki związkowej w zadeklarowanej przez nich wysokości, stałej dla wszystkich członków, oraz przekazywanie imiennej listy pracowników wraz z kwotą tej składki, nie narusza przepisów o ochronie danych osobowych. Natomiast, jeżeli wysokość składki stanowi określoną wartość procentową wynagrodzenia pracownika i jej wskazanie umożliwi określenie wysokości wynagrodzenia konkretnego pracownika, to przekazywanie takiej informacji, w ocenie organu właściwego do spraw ochrony danych osobowych, jest sprzeczne z zasadami ochrony danych określonymi w art. 5 ust. 1 RODO oraz przepisami o ochronie danych osobowych, ponieważ w ten sposób pracodawca pośrednio ujawnia informację o wysokości wynagrodzenia pracownika[193].

Przetwarzanie danych osobowych kandydata do pracy w zakresie toczącego się postępowania karnego.

Prezes UODO udzielał także odpowiedzi na pytanie, czy pracodawca ma prawo żądać od kandydata do pracy informacji o toczących się i niezakończonych postępowaniach karnych. W odpowiedzi organ wskazał, że zgodnie z art. 22^1 Kodeksu Pracy, katalog danych, które mogą być przetwarzane przez pracodawcę jest zamknięty i pracodawca nie może przetwarzać danych, które wykraczają poza ten zakres. Informacja o toczącym się postępowaniu karnym nie stanowi informacji, do której mocą ustawy ma dostęp pracodawca. Nie może on żądać od osoby ubiegającej się o zatrudnienie informacji na temat ewentualnych toczących się postępowań karnych oraz informacji o ich przebiegu. Informacja o toczącym się postępowaniu karnym nie oznacza, że dana osoba będzie skazana. Taka informacja nie jest również zawarta w Krajowym Rejestrze Karnym,

[193] ZSZZS.027.39.2019

ponieważ rejestr zawiera informacje m.in. o osobach prawomocnie skazanych oraz przeciwko którym prawomocnie umorzono postępowanie karne. Pracodawca jest jednak podmiotem uprawnionym do pozyskiwania informacji z Krajowego Rejestru Karnego w zakresie niezbędnym dla zatrudnienia pracownika, co do którego z przepisów ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej[194].

Udostępnianie przez szkoły informacji w ramach dostępu do informacji publicznej.

W odpowiedzi na pytanie dotyczące udostępniania przez szkoły informacji w ramach dostępu do informacji publicznej, Prezes UODO przypomniał, że ostateczne rozstrzygnięcie sprawy z zakresu dostępu do informacji publicznej nie należy do organu do spraw ochrony danych osobowych. Decyzja o tym, czy informacja ma charakter publiczny, czy dokonać jej udostępnienia czy też nie, należy do dysponującego informacją, a więc w tym przypadku do szkoły.

Podmiot udostępniający informację publiczną musi w każdym przypadku rozważyć, czy informacje, które udostępnia nie będą naruszały prywatności osoby, której dane dotyczą. W sytuacji, kiedy udostępnienie dokumentów, w tym danych osobowych będzie naruszało prywatność osoby, której dane dotyczą, wówczas podmiot będący dysponentem informacji publicznej będzie zobowiązany do zanonimizowania tych danych osobowych, których przetwarzanie będzie naruszało prawo do ochrony danych osobowych[195].

Postępowanie z aktami osobowymi pracowników w razie przeniesienia pracownika.

W odpowiedzi na pismo jednego z urzędów centralnych, Prezes UODO przedstawił swoje stanowisko dotyczące przetwarzania danych osobowych w aktach pracowniczych w razie przeniesienia urzędnika służby cywilnej oraz pracownika służby cywilnej do innego urzędu. Stosownie do art. 75 ustawy o służbie cywilnej urząd, z którego urzędnik służby cywilnej oraz pracownik służby cywilnej został przeniesiony, przekazuje do urzędu, w którym urzędnik służby cywilnej oraz pracownik służby cywilnej ma być zatrudniony, akta osobowe wraz z pozostałą dokumentacją w sprawach związanych ze stosunkiem pracy tych osób. Zatem urząd zatrudniający urzędnika służby cywilnej oraz pracownika służby cywilnej ma obowiązek przyjąć przekazywane z innego urzędu akta osobowe wraz z pozostałą dokumentacją w sprawach związanych ze

[194] ZSZZS.027.217.2019
[195] ZSZZS.027.203.2019

stosunkiem pracy urzędnika służby cywilnej oraz pracownika służby cywilnej i nie ma możliwości odmowy ich przyjęcia, tym bardziej powołując się na przepisy o ochronie danych osobowych. Urząd przyjmujący akta osobowe wraz z pozostałą dokumentacją w sprawach związanych ze stosunkiem pracy nie ma prawa do usuwania z akt osobowych pracownika jakichkolwiek dokumentów dotyczących zakończonego stosunku pracy. Powyższy artykuł, jak i inne przepisy ustawy o służbie cywilnej, nie uprawniają urzędu zatrudniającego przenoszonego urzędnika służby cywilnej oraz pracownika służby cywilnej do zwrócenia akt osobowych pracownika do dotychczasowego pracodawcy. Artykuł 9 ustawy o służbie cywilnej stanowi ponadto, że w sprawach dotyczących stosunku pracy w służbie cywilnej, nieuregulowanych w tej ustawie, stosuje się przepisy Kodeksu pracy i inne przepisy prawa pracy. A zatem urząd przyjmujący przenoszonego urzędnika służby cywilnej oraz pracownika służby cywilnej do przekazanych akt osobowych oraz pozostałej dokumentacji w sprawach związanych ze stosunkiem pracy powinien stosować odpowiednio rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej[196].

W odniesieniu do akt osobowych pracownika urząd administracji rządowej, którego pracownicy należą do Korpusu służby cywilnej, powinien być traktowany jako pracodawca w rozumieniu Kodeksu pracy. W związku z tym urząd ten odpowiada za prawidłowość prowadzenia takiej dokumentacji, np. w przypadku udzielenia kary porządkowej pracownikowi na podstawie art. 108 Kodeksu pracy, przed migracją pracownika, a gdy do jej zatarcia dochodzi już po migracji, to jednostka przyjmująca powinna usunąć z akt osobowych pracownika informacje o karze.

Przetwarzanie informacji o szczepieniach

Prezes UODO w związku z otrzymanym zapytaniem zajął także stanowisko dotyczące kwalifikacji danych osobowych dotyczących szczepień ochronnych dziecka, jako danych osobowych szczególnej kategorii oraz dopuszczalności obligowania rodziców do przekazywania informacji o odbytych szczepieniach ochronnych dzieci bądź przedstawiania zaświadczeń lekarskich, które usprawiedliwiają brak ich wykonania. Zapytanie skierowane było do organu w związku z informacją o zamiarze podjęcia przez władze miasta uchwały wprowadzającej w postępowaniu rekrutacyjnym do publicznych przedszkoli i oddziałów przedszkolnych w szkołach

[196] Dz. U. z 2018 r. poz. 2369

podstawowych m.in. kryterium dotyczącego podania informacji o poddaniu dziecka obowiązkowym szczepieniom ochronnym.

W odpowiedzi organ wskazał, że przetwarzanie informacji o odbytych szczepieniach dotyczy danych dotyczących zdrowia, czyli zgodnie z RODO – szczególnej kategorii danych, które powinny zostać objęte większą ochroną. W art. 131 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe, ustawodawca przewidział kryteria, które należy brać pod uwagę w ramach prowadzenia postępowania rekrutacyjnego do publicznego przedszkola, oddziału przedszkolnego w publicznej szkole podstawowej lub publicznej innej formie wychowania przedszkolnego. Dopiero na drugim etapie rekrutacji ustawodawca przewiduje uprawnienie dla organu prowadzącego do określenia dodatkowych kryteriów, które mogłyby być zastosowane w przypadku, gdy kandydaci do ww. placówki uzyskają równorzędne wyniki. W przypadku katalogu informacji wymienionych w ust. 2 ww. przepisu, podmiot prowadzący rekrutację jest uprawniony do przetwarzania danych o stanie zdrowia kandydata lub jego rodziców w związku z przesłankami określonymi w art. 9 ust. 2 RODO. Jednakże przetwarzanie danych o stanie zdrowia innych niż wymienione w art. 131 ust. 2 ustawy Prawo oświatowe jest niedopuszczalne. W ocenie Prezesa informacja o szczepieniu kandydata nie mieści się w ww. katalogu, w związku z czym należy przyjąć, że w przedmiotowej sprawie nie występuje żadna z przesłanek określonych w art. 9 ust. 2 RODO legalizująca pozyskiwanie tego rodzaju danych osobowych.

Odnosząc się natomiast do kwestii przetwarzania ww. informacji w ramach ubiegania się o objęcie dziecka opieką w żłobku lub klubie dziecięcym albo przez dziennego opiekuna wskazać należy, że ustawodawca w art. 3a ust. 1 pkt 6 ustawy z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3 przewidział, że rodzic dziecka powinien przekazać podmiotowi prowadzącemu ww. opiekę dane osobowe w zakresie informacji o stanie zdrowia, jednakże mogą być one przetwarzane wyłącznie w związku z rekrutacją oraz w zakresie i celu zapewnienia dziecku prawidłowej opieki (art. 3a ust. 2 ww. ustawy). Prezes UODO wskazał, że okoliczność zaszczepienia dziecka nie ma znaczenia dla zapewnienia mu prawidłowej opieki. Oznacza to, że przetwarzanie danych osobowych dzieci w zakresie informacji o wykonaniu w stosunku do nich obowiązku szczepień ochronnych, nie może stanowić informacji wymaganej przez podmiot prowadzący żłobek lub klub dziecięcy oraz podmiot zatrudniający dziennego opiekuna na etapie rekrutacji. Wymaganie przez władze samorządowe, w ramach postępowania rekrutacyjnego do przedszkoli i szkół, od rodziców przedstawienia informacji o odbytych szczepieniach oraz zaświadczenia lekarskiego dotyczącego ewentualnych przeciwwskazań usprawiedliwiających brak

obowiązkowych szczepień ochronnych u dziecka nie znajduje podstawy prawnej i pozostaje w sprzeczności z przepisami o ochronie danych osobowych[197].

Wykonywanie kserokopii orzeczenia o stopniu niepełnosprawności lub legitymacji osoby niepełnosprawnej przez podmioty lecznicze, w celu umożliwienia skorzystania ze świadczeń poza kolejnością.

Kwestie dotyczące szczególnych uprawnień do korzystania ze świadczeń poza kolejnością regulują przepisy ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Zgodnie z art. 47c ust. 1 tej ustawy, świadczeniobiorcy m.in. posiadający orzeczenie o znacznym stopniu niepełnosprawności, mają prawo do korzystania poza kolejnością ze świadczeń opieki zdrowotnej oraz z usług farmaceutycznych udzielanych w aptekach. Szczególne uprawnienia przysługują na podstawie dokumentu, który do tego uprawnia. Prezes UODO odpowiadając na to pytanie prawne wskazał również, że przytoczony przepis wskazuje jedynie na kategorie podmiotów, którym przysługują określone uprawnienia. Nie daje on natomiast podstawy do przetwarzania danych osobowych tych osób poprzez sporządzanie kopii dokumentów uprawniających do skorzystania z tych szczególnych uprawnień. Oznacza to, że weryfikacja tego, czy dana osoba posiada szczególne uprawnienia, czy też nie, powinna odbywać się wyłącznie na podstawie okazania dokumentu, który te uprawnienia potwierdza[198].

Udostępnianie danych osobowych innym instytucjom publicznym.

Z kolei **podmioty z sektora publicznego** bardzo często pytały o dopuszczalność udostępniania danych osobowych innym instytucjom publicznym. Przykładem może być pytanie Ośrodka Pomocy Społecznej dotyczące możliwości udostępnienia danych osobowych zawartych w dokumentacji podopiecznych tej placówki na rzecz urzędu miasta[199]. Za przesłankę legalizującą udostępnienie danych osobowych urząd miasta uznał art. 6 ust. 1 lit. e RODO, który stanowi, że przetwarzanie jest zgodne z prawem wówczas, gdy „jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi", lecz nie wskazał przepisów rangi ustawy stanowiących podstawę realizacji zadań i celów, w jakich miało nastąpić udostępnienie. W odpowiedzi organ nadzorczy wskazał, że co do zasady działanie podmiotów publicznych odbywa się wyłącznie na podstawie i w granicach prawa, co zostało unormowane w art. 7 Konstytucji RP. Występowanie z wnioskiem

[197] ZSZZS.027.146.2019
[198] ZSZZS.027.131.2019
[199] ZSPU.027.322.2019.EKR

o udostępnienie danych osobowych wyłącznie na podstawie przepisów RODO, nie znajduje zatem uzasadnienia prawnego, gdyż to nie RODO, lecz krajowe przepisy szczególne stanowią o kompetencjach tych organów i sposobie ich realizacji. Zatem w pierwszej kolejności to te przepisy powinny być wskazywane jako przesłanka legalizująca pozyskiwanie danych. Wyjaśniając te wątpliwości Prezes UODO wskazał dodatkowo na art. 100 ust. 1 ustawy z dnia 12 marca 2004 r. o pomocy społecznej[200] i wynikającą z niego niedopuszczalność ujawniania informacji z postępowań administracyjnych prowadzonych przez ośrodki pomocy społecznej na rzecz wszelkich podmiotów, w tym innych organów administracji publicznej – o ile nie ma wyraźnej podstawy ustawowej. W ocenie organu nadzorczego powoływanie się na przesłankę legalności przetwarzania danych określoną w art. 6 ust. 1 lit. e RODO, tj. zgodność przetwarzania z prawem, jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, bez wskazania także przepisów rangi ustawy stanowiących podstawę realizacji wyżej wymienionych zadań i celu, w omawianym przypadku jest niedopuszczalne.

Wiele pytań od podmiotów z sektora publicznego dotyczyło też przetwarzania danych osobowych w związku z dostępem do informacji publicznej. Wątpliwości budziły także kwestie związane z rolą poszczególnych podmiotów w procesie przetwarzania danych osobowych – kto w konkretnym przypadku jest administratorem, a kto podmiotem przetwarzającym, jaki podmiot może być uznany za współadministratora.

Jednocześnie warto pokreślić, że tylko w nielicznych przypadkach do pytań nadsyłanych do Urzędu Ochrony Danych Osobowych przez podmioty z sektora publicznego dołączane były opinie powołanego w ich strukturach inspektora ochrony danych (IOD), co należy uznać za nieprawidłową praktykę. Zgodnie z przyjętymi w RODO rozwiązaniami, IOD (którego wyznaczenie w jednostkach sektora finansów publicznych jest obowiązkowe[201]) ma być nie tylko doradcą dla administratora, ale także pełnić rolę punktu kontaktowego, a więc m.in. być pośrednikiem między nim a organem nadzorczym. Dlatego w budzących wątpliwości sytuacjach związanych z przetwarzaniem danych osobowych, administrator w pierwszej kolejności powinien zwrócić się do IOD. To jego zadaniem jest poddanie danego przypadku szczegółowej analizie i przedstawienie opinii na ten temat. W uzasadnionych przypadkach to IOD może zwrócić się do UODO z prośbą o konsultacje. Zgodnie bowiem z art. 57 ust. 3 RODO, zadaniem organu nadzorczego jest bezpłatne wypełnianie zadań na

[200] Dz. U. z 2018 r. poz. 1508 z późn. zm.
[201] Więcej na stronie internetowej UODO: https://uodo.gov.pl/pl/223/638 .

rzecz osoby, której dane dotyczą, i – gdy ma to zastosowanie – inspektora ochrony danych. Na kwestię tę Prezes UODO zwrócił uwagę m.in. w Newsletterze UODO dla inspektorów ochrony danych numer 6/2019. Jednocześnie wskazał tam, że „wiążące zaopiniowanie przez UODO konkretnych rozwiązań wyłącznie na podstawie przesłanej korespondencji, która dodatkowo w niepełny sposób opisuje ewentualne czynności wykonywane na danych osobowych, nie jest możliwe. Co do zasady Prezes UODO – stosownie do zadań określonych w art. 57 RODO – bada i kontroluje procesy przetwarzania danych osobowych w ramach prowadzonych postępowań administracyjnych. Jego wiążące stanowisko w konkretnej sprawie dotyczącej przetwarzania danych osobowych powinno być zawarte w treści decyzji administracyjnej, na podstawie zebranego materiału dowodowego".

Pytania od podmiotów z sektora mieszkalnictwa były nadsyłane zarówno przez zarządców nieruchomości, jak i przez członków wspólnot oraz spółdzielni mieszkaniowych. Dotyczyły przede wszystkim przetwarzania danych osobowych w związku z zarządzaniem nieruchomościami, w tym ich udostępniania określonym podmiotom i osobom, a także stosowania monitoringu wizyjnego.

Z pytaniem dotyczącym monitorowania zwróciła się do UODO jedna ze spółdzielni mieszkaniowych[202] w związku z wątpliwościami, czy prowadzona w telewizji lokalnej transmisja obrad organów spółdzielni nie naruszyła prawa ochrony danych osobowych. Organ nadzorczy wskazał, że zgodnie z wyrażoną w art. 5 ust. 1 lit. c RODO zasadą minimalizacji danych, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Art. 81 ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych stanowi, że członek spółdzielni mieszkaniowej ma prawo otrzymania odpisu statutu i regulaminów oraz kopii uchwał organów spółdzielni i protokołów obrad organów spółdzielni, protokołów lustracji, rocznych sprawozdań finansowych oraz faktur i umów zawieranych przez spółdzielnię z osobami trzecimi. Tym samym udostępnienie danych osobowych zawartych w protokole obrad organów spółdzielni ma umocowanie w ustawie z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych i jest zgodne z prawem, gdyż jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO). Natomiast udostępnienie obrad organów spółdzielni mieszkaniowej w postaci transmisji w telewizji lokalnej nie ma bezpośredniego oparcia w ustawie z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych. Analizy wymaga również, czy dla zaspokojenia potrzeb członków spółdzielni konieczne i adekwatne jest udostępnianie danych osobowych w ramach transmisji obrad organów

[202] ZSPU.027.109.2019

spółdzielni. Dla ochrony praw osób, których dane są przetwarzane, spółdzielnia mieszkaniowa – jako ich administrator – powinna tak określić procedury postępowania w związku z transmisją i nagrywaniem obrad, aby należycie je chronić, zwłaszcza dane należące do szczególnych kategorii wskazanych w art. 9 i 10 RODO (np. poprzez ich anonimizację).

Podsumowując, zakres tematyczny pytań prawnych kierowanych do Urzędu był bardzo szeroki i dotyczył różnych aspektów przetwarzania danych osobowych. Wątpliwości dotyczyły nie tylko stosowania RODO, ale także innych, szczególnych przepisów prawa. Wskazać można, że w szczególności podmioty z sektora administracji publicznej dość dobrze sprostały określonym w RODO obowiązkom. Wiele podmiotów we właściwy sposób dopełniło obowiązek informacyjny, dobrze radziło sobie z doborem środków zapewniających bezpieczeństwo danych osobowych, a nawet zaczęło wdrażać zasady ochrony danych osobowych już na etapie projektowania określonych rozwiązań, czego dowodzą kontrole i prezentowane UODO analizy ryzyka i oceny skutków, np. dla monitoringu miejskiego. Nawet zarejestrowana duża liczba zgłoszeń naruszeń ochrony danych osobowych może być również dowodem na spełnienie obowiązku informacyjnego wobec osób, których dane osobowe zostały naruszone. Świadczy to jednocześnie o właściwym podejściu do tego nowego, wprowadzonego przez RODO rozwiązania. Powyższe działania, zwłaszcza właściwe komunikowanie się z podmiotami danych, przyczyniają się jednocześnie do wzrostu świadomości obywateli, przez co w 2019 r. wzrost liczby skarg i pytań kierowanych do Prezesa UODO nie jest już tak lawinowy, jak w roku ubiegłym.

Niemniej w codziennej praktyce Urzędu zdarzają się problemy z właściwym stosowaniem RODO, które częściowo wynikają z niespójności lub niejasności przepisów sektorowych. Dlatego Prezes UODO podejmuje działania mające na celu ich eliminację, jak np. przygotowywanie materiałów informacyjno-edukacyjnych, czy kierowanie wystąpień o rozważenie stosownych zmian prawa. Instrumentem pomocnym w zapewnieniu zgodności z RODO mogą być także wspomniane wcześniej kodeksy postępowania. Ich celem jest pomoc we właściwym stosowaniu przepisów RODO poprzez doprecyzowanie jego zastosowania z uwzględnieniem specyfiki danego sektora. Mogą więc być pewnego rodzaju instrukcjami działania, np. w zakresie sposobu dokonywania operacji zbierania danych czy spełniania różnych obowiązków. Dotyczyć to może zwłaszcza tych przypadków, kiedy wymogi dotyczące ochrony danych nie są wystarczająco szczegółowe i wymagają doprecyzowania, bądź kiedy są uszczegóławiane na mocy innych przepisów. Prezes UODO wspiera wszystkie środowiska (prywatne i publiczne), które zdecydują się na opracowanie takiego dokumentu.

Organ nadzorczy odpowiadał na pytania prawne w formie indywidualnej, a w przypadku zagadnień budzących wyjątkowe zainteresowanie społeczne – dodatkowo umieszczał wyjaśnienia na stronie internetowej UODO. Jako przykład podać można zalecenia dotyczące przetwarzania danych w wyborach parlamentarnych – 13 października 2019 r.[203] oraz zalecenia dotyczące nagrywania i transmisji z posiedzeń w jednostkach samorządu terytorialnego[204]. Wydawał także **komunikaty** wyjaśniające stanowisko organu odnośnie istotnych kwestii, np. dotyczących ochrony danych w sektorze szkolnictwa (zob. komunikat dot. braku podstaw prawnych do przetwarzania w SIO informacji o tym, że dany nauczyciel strajkuje), czy zatrudnienia (komunikat dot. braku podstaw prawnych do przeprowadzania samodzielnie przez pracodawcę kontroli stanu trzeźwości pracowników). Wszystkie te działania mają na celu ułatwienie stosowania przepisów prawa o ochronie danych osobowych w praktyce.

12.2. Wystąpienia

Istotną rolę w kształtowaniu i podnoszeniu poziomu ochrony danych osobowych mają wystąpienia Prezesa Urzędu Ochrony Danych Osobowych, w których zawarte były wnioski o zmianę obowiązujących regulacji prawnych lub o wprowadzenie nowych norm dotyczących przetwarzania danych osobowych, a także zmianę praktyk w podmiotach, do których wystąpienia te były kierowane.

Poniżej przedstawione zostały wybrane przykłady wystąpień Prezesa UODO do podmiotów administracji publicznej i podmiotów prywatnych działających w różnych sektorach.

Art. 70a Prawa bankowego po 4 maja 2019 r.

W 2019 r. Prezes UODO wystąpił z pismem do Przewodniczącego KNF oraz do Prezesa ZBP[205] o udzielenie informacji w związku z nowym – obowiązującym od dnia 4 maja 2019 r. – art. 70a Prawa bankowego. Zgodnie z tym przepisem klienci banków i innych instytucji upoważnionych do udzielania kredytów, mają prawo do uzyskania informacji na temat czynników, w tym danych osobowych wnioskującego, które miały wpływ na dokonaną ocenę zdolności kredytowej. Przepis art. 70a ust. 1 Prawa bankowego stanowi, że wyjaśnienia dotyczące oceny zdolności kredytowej mają być udzielane na wniosek. Dotyczy to informacji na temat wszystkich produktów kredytowych dla klienta indywidualnego: kredytów i pożyczek hipotecznych, pożyczek

[203] https://uodo.gov.pl/pl/138/1217
[204] https://uodo.gov.pl/pl/138/1258
[205] ZSPR.027.414.2019

gotówkowych, kart kredytowych, limitów odnawialnych oraz produktów kredytowych kierowanych do firm i przedsiębiorców. Inny przepis Prawa bankowego uzależnia natomiast prawo do podejmowania przez banki zautomatyzowanych decyzji kredytowych (w tym profilowania) od zagwarantowania klientowi prawa do otrzymania stosownych wyjaśnień, co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska (art. 105a ust. 1a Prawa bankowego). Przepis ten ogranicza jednocześnie katalog danych, z których może korzystać bank dla realizacji podejmowania zautomatyzowanych decyzji kredytowych (art. 105a ust. 1b-1c Prawa bankowego). Artykuł 10 ust. 2 ustawy o kredycie konsumenckim stanowi, że jeżeli kredytodawca odmówi konsumentowi udzielenia kredytu konsumenckiego, przepisy art. 70a ust. 1 i 2 Prawa bankowego stosuje się odpowiednio. Przepisy nie określają jednak terminu ani zakresu, w którym klient może wnioskować o przedmiotowe informacje. O wyjaśnienia można wystąpić w przypadku, gdy decyzja kredytowa zostanie wydana, a z dodatkowego prawa do wyjaśnienia podstaw decyzji podjętej automatycznie można skorzystać po jej podjęciu.

Z powyższych względów Prezes UODO zwrócił się do Komisji Nadzoru Finansowego i Związku Banków Polskich z pytaniami dotyczącymi praktyki banków w zakresie uwzględniania uprawnienia wynikającego z art. 70a Prawa bankowego. Poprosił o wyjaśnienie, czy w zakresie tego uprawnienia zostały zapewnione przez banki jednolite standardy postępowania, w tym w szczególności w zakresie terminów jego realizacji. Ponadto zapytał, czy Komisja Nadzoru Finansowego lub Związek Banków Polskich przekazali bankom rekomendacje dotyczące realizacji ww. prawa.

Pozyskiwanie zgód na przetwarzanie danych osobowych

Prezes Urzędu Ochrony Danych Osobowych – po uzyskaniu informacji od Prezesa Urzędu Ochrony Konkurencji i Konsumentów wskazującej na naruszenie przez spółkę przepisów RODO w zakresie pozyskiwania zgody na przetwarzanie danych osobowych zgodnie z ofertą „Prąd dla dużej rodziny" – skierował do tego podmiotu wystąpienie dotyczące zgód marketingowych.

W przedmiotowej ofercie spółki pole *Akceptuję zgody marketingowe* było polem wymaganym w zakresie obowiązkowego zaakceptowania przez odbiorcę zgód marketingowych. Organ nadzorczy wskazał, że za niepożądaną uznaje się sytuację łączenia zgody z akceptacją warunków lub uzależniania wykonania umowy lub świadczenia usługi od uwzględnienia wniosku o wyrażenie zgody na przetwarzanie danych osobowych, które nie jest konieczne w celu wykonania umowy lub świadczenia usługi. Administrator musi mieć świadomość, że zgody nie można uzyskać

w drodze tej samej czynności, co zawarcie umowy czy zaakceptowanie ogólnych warunków usługi. Zbiorczego zaakceptowania ogólnych warunków nie można uznać za wyraźne działanie potwierdzające wyrażenie zgody na wykorzystanie danych osobowych. Jeżeli wyrażenie zgody stanowi nieodłączną i niepodlegającą negocjacji część warunków umowy, uznaje się, że nie jest ona dobrowolna. Zgoda nie może być dorozumiana z oświadczeń innej treści, milcząca (niepodjęcie działań nie może oznaczać zgody) lub wynikać z działania polegającego na domyślnym zaznaczeniu okienek przez podmiot danych. Pozyskane przez administratora zgody muszą spełniać kryteria opisane w art. 4 pkt 11 (dobrowolności, konkretności, świadomości i jednoznaczności), art. 6 ust. 1 lit. a w związku z art. 7 oraz art. 9 ust. 2 lit. a RODO.

Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu

Prezes Urzędu Ochrony Danych Osobowych zwrócił się do Generalnego Inspektora Informacji Finansowej[206] – jako organu właściwego w sprawach przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu – o przedstawienie stanowiska, jakimi środkami instytucje obowiązane, o których mowa w art. 2 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, powinny dokonywać identyfikacji klienta i czy w każdym przypadku instytucje te powinny pozyskiwać od klientów kopie dokumentów, w tym dokumentów tożsamości. Impulsem do niniejszego wystąpienia były liczne wątpliwości, jakie pojawiły się wraz z wejściem w życie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[207]. Ustawa ta nałożyła na niektóre podmioty (tzw. instytucje obowiązane) obowiązek stosowania środków bezpieczeństwa finansowego, w tym obowiązek identyfikacji klienta. Do Urzędu Ochrony Danych Osobowych wpływały sygnały od osób zaniepokojonych wymogiem udostępniania bankom, przedsiębiorstwom świadczącym usługi płatnicze i innym podmiotom, powołującym się na obowiązki wynikające z przywołanej ustawy, kopii dokumentów tożsamości (w tym np. zdjęcia twarzy, tzw. selfie z dokumentem tożsamości w ręce), a także innych dokumentów, przykładowo rachunków za zużycie energii elektrycznej, czy kopii umowy z rachunku bankowego, itd. Wątpliwości klientów obligowanych do przedkładania kopii dokumentów tożsamości i innych dokumentów zawierających ich dane osobowe oraz aktualności wynikających z tych informacji były spowodowane obawą posłużenia się ich tożsamością przez osoby nieuprawnione do wykorzystania w innych celach. Zgodnie z przepisami ustawy

[206] ZSPR.027.363.2019

[207] Dz.U. z 2019 r. poz.1115 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu.

o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, instytucje obowiązane, wskazane w art. 2 tej ustawy, stosują środki bezpieczeństwa określone w art. 34, które obejmują m.in. identyfikację klienta. W myśl art. 34 ust.4 tego aktu prawnego instytucje obowiązane mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie. W opinii Prezesa Urzędu Ochrony Danych Osobowych stosowanie środków bezpieczeństwa przez instytucje obowiązane, do których należy m.in. weryfikacja tożsamości poprzez kopiowanie dokumentów tożsamości, powinno mieć miejsce jedynie w sytuacjach, gdy zachodzą przesłanki do takiego stosowania. Przesłanki te zostały natomiast wprost określone w art. 35 przedmiotowej ustawy. Pozostaje zatem uzasadniona wątpliwość, czy żądanie przedstawiania kopii lub kopiowanie dowodów tożsamości i innych dokumentów zawierających dane osobowe przez instytucje obowiązane w sytuacjach innych niż wskazane w art. 35 tej ustawy, ma podstawy prawne. Art. 34 ust. 1 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, określający środki bezpieczeństwa finansowego, stanowi, że środkiem tym jest m.in. identyfikacja klienta oraz weryfikacja jego tożsamości (art. 34 ust. 1 pkt 1), nie zaś kopiowanie dokumentu tożsamości. Kopiowanie należy uznać za uprawnienie przysługujące podmiotom obowiązanym w oparciu o przepis art. 34 ust. 1, który mówi o możliwości stosowania przez podmioty takiego narzędzia *„instytucje na potrzeby stosowania środków bezpieczeństwa finansowego mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie"*. Nie można zatem uznać, że na podmiotach obowiązanych leży obowiązek każdorazowego kopiowania dokumentów tożsamości, ale że podmioty te mają prawo z takiego instrumentu korzystać. Każdorazowa decyzja o skopiowaniu dokumentu tożsamości, czy też żądanie przedstawienia takich kopii, powinna być poprzedzona analizą i zweryfikowaniem, czy rzeczywiście taka czynność jest niezbędna, z uwzględnieniem przepisów RODO, w szczególności w zgodzie z zasadami celowości i minimalizacji, o których mowa w art. 5 ust. 1 lit. b i c tego rozporządzenia. Organ nadzorczy podkreślił, że to Generalny Inspektor Informacji Finansowej weryfikuje i ocenia, czy podmioty obowiązane prawidłowo realizują obowiązki przewidziane w przywołanej ustawie w zakresie środka bezpieczeństwa, jakim jest identyfikacja klienta i rozlicza ich z wypełnienia tych obowiązków. **Istotnym jest jego stanowisko – czy organ ten oczekuje od instytucji obowiązanych przedkładania – jako potwierdzenie wypełnienia obowiązku identyfikacji klienta – kserokopii dokumentów tożsamości**, ewentualnie innych dokumentów celem ich potwierdzenia.

Organ nadzorczy stoi na stanowisku, że kopiowanie można uznać za legalne, jeżeli wymagają tego względy bezpieczeństwa określone w art. 35 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (przesłanki stosowania środków bezpieczeństwa). Banki podczas dokonywania oceny poziomu ryzyka, o której mowa w art. 33 tej ustawy, powinny każdorazowo brać pod uwagę zasady: celowości i minimalizacji danych ustanowionych przepisami RODO, tak aby pozyskiwanie kopii dokumentów tożsamości odbywało się tylko w uzasadnionych przypadkach i w konkretnym celu, a nie „na zapas". Wewnętrzne procedury banków związane ze stosowaniem środków bezpieczeństwa finansowego powinny uwzględniać powyższe regulacje. Przy opracowywaniu procedur warto także pamiętać o zasadzie ograniczenia czasowego wynikającej z art. 5 ust. 1 pkt e RODO, zgodnie z którą dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane są przetwarzane.

Wycieki danych z banków

W związku z pojawiającymi się sygnałami o niezgodnych z prawem praktykach pracowników banków, polegających na nielegalnym sprzedawaniu baz danych klientów banków, w tym potencjalnie na to wskazującymi ogłoszeniami na portalach takich jak: oferta24.info, sprzedajemy.pl, itd., Prezes Urzędu Ochrony Danych Osobowych skierował do Prezesa Związków Banków Polskich oraz do Przewodniczącego Komisji Nadzoru Finansowego wystąpienie[208] o przekazanie informacji, czy podmioty te, jako organy sprawujące nadzór nad rynkiem finansowym, podjęły lub rozważają podjąć działania, które przyczyniłyby się do zminimalizowania zjawiska nielegalnego wykorzystywania przez pracowników banków danych osobowych klientów.

Prezes Urzędu Ochrony Danych Osobowych zwrócił uwagę, że handel danymi osobowymi (bazami je zawierającymi) jest niebezpiecznym zjawiskiem, które występuje na tzw. czarnym rynku. Nielegalnie pozyskane dane osobowe mogą być wykorzystywane nie tylko w celach przedstawiania niechcianych ofert marketingowych, ale także do zaciągania zobowiązań finansowych na cudze konto, oczywiście bez wiedzy i zgody osób, których dane dotyczą. Przyczyną wycieków może być brak mechanizmów zabezpieczania danych czy też ich niewłaściwe lub nieskuteczne wdrożenie przez administratorów. Osobami, które przyczyniają się do wycieku danych osobowych oraz do nielegalnego obrotu tymi danymi są nierzadko pracownicy podmiotów posiadających takie dane, zwłaszcza osoby kończące współpracę z tymi podmiotami. Dotyczy to

[208] ZSPR.027.431.2019

także pracowników banków. W wielu przypadkach do udostępniania danych przez pracowników dochodzi w wyniku błędu, stosowania niewłaściwych środków ostrożności, czasem jednak także poprzez zamierzone działania.

Organ nadzorczy zaznaczył, że pracownicy dopuszczający się naruszeń polegających na nielegalnym udostępnianiu danych osobowych, czy też inne osoby winne w tym zakresie za działania/zaniechania niezgodne z prawem, powinny ponosić odpowiedzialność przewidzianą przepisami prawa. Istotne jest jednak także to, jakie działania podejmują banki, aby takim sytuacjom zapobiegać. Nie tylko, czy wyciągają konsekwencje wobec pracowników nieprzestrzegających zasad ochrony danych osobowych, ale także czy wprowadziły i stosują rozwiązania systemowe w tym zakresie. Z punktu widzenia ochrony danych osobowych oraz ochrony tajemnicy bankowej, niedopuszczalne jest przenoszenie czy przesyłanie przez pracowników banków danych osobowych klientów na prywatne skrzynki mailowe czy nośniki danych osobowych. Nawet jeśli pracownik nie zamierza w nielegalny sposób wykorzystywać baz danych, które zgrał na prywatny nośnik danych lub przesłał na prywatną skrzynkę pocztową, ryzyko związane z naruszeniem bezpieczeństwa danych, niewłaściwym ich wykorzystaniem czy ich utratą, jest wysokie. W związku z powyższym istotne jest, aby banki kontrolowały pracowników pod kątem przestrzegania przez nich procedur ochrony danych osobowych, a także rozliczały w tym zakresie pracowników – zarówno w trakcie trwania stosunku pracy, jak i w okresach wypowiedzenia stosunku pracy – a także odpowiednio, systematycznie i skutecznie szkoliły pracowników z zakresu ochrony danych osobowych. Banki – jako instytucje zaufania publicznego – powinny dbać o wymienione wyżej kwestie, w tym właściwe zabezpieczenie danych osobowych i chronić je w sposób szczególny, co wynika ze zobowiązania nałożonego mocą art. 104 Prawa bankowego do zachowywana tajemnicy bankowej. Zatem bank nie może ujawniać informacji objętych tajemnicą innym podmiotom, chyba że klient banku zgodzi się, aby te informacje przekazać.

Wystąpienie do Poczty Polskiej

Prezes Urzędu Ochrony Danych Osobowych skierował wystąpienie do Prezesa Poczty Polskiej S.A.[209] w związku z pozyskaniem informacji o przyjętych przez ten podmiot regulacjach wewnętrznych określających procedurę realizowania wpłat na rachunek bankowy.

[209] ZSPR.027.98.2019

Z postanowień regulaminu dotyczącego wpłaty na rachunek bankowy wynikało, że realizacja przekazu pieniężnego za pośrednictwem Poczty Polskiej możliwa jest w formie – wskazywanej jako bardziej dogodna dla klienta – „zlecenia ustnego" pracownikowi poczty na taki przekaz. W trakcie realizacji przekazu, o ile klient wybiera tzw. werbalne przekazanie informacji, osoby przebywające w danej placówce pocztowej mogą usłyszeć informacje niezbędne do wykonania przelewu, tj. dane osobowe osoby wykonującej przelew oraz dane osobowe odbiorcy przelewu, a także kwotę, na jaką jest on realizowany. Organ nadzorczy wskazał, że niezbędne jest jak najszybsze wyeliminowanie rozwiązań mogących być przyczyną przetwarzania przez Pocztę Polską danych osobowych jej klientów niezgodnie z przepisami o ochronie danych osobowych i wdrożenie przez Pocztę Polską rozwiązań, które dadzą gwarancję właściwej ochrony danych osobowych przez nią przetwarzanych. Poczta Polska powinna powtórnie przeanalizować, czy przyjęta możliwość zleceń ustnych powinna być realizowana, czy raczej powinna następować w wyjątkowych sytuacjach, a nie być zasadą.

W odpowiedzi na wystąpienie Prezesa Urzędu Ochrony Danych Osobowych, Prezes Poczty Polskiej poinformował, że nie mając możliwości wydzielania w placówkach pocztowych oddzielnych pomieszczeń do przekazywania danych w formie werbalnej, podjęto działania mające na celu ograniczenie ryzyka naruszenia danych osobowych, w tym m.in.: zmieniony został *Regulamin świadczenia usługi finansowej przyjmowania wpłat na rachunki bankowe w Poczcie Polskiej S.A. w obrocie krajowym (*w zakresie braku wskazywania wpłat na rachunki bankowe w Poczcie Polskiej S.A.), skierowano komunikat do pracowników odpowiedzialnych za przyjmowanie wpłat, dotyczący obowiązku wskazywania klientom preferowanych, bezpiecznych form przekazywania danych osobowych oraz zaplanowano działania szkoleniowe dla pracowników.

Rachunki uśpione

Prezes UODO ponownie zwrócił się do Ministra Finansów o podjęcie działań mających na celu wprowadzenie zmian w ustawie z dnia 29 sierpnia 1997 r. Prawo bankowe i ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, zapewniających zgodność unormowań dotyczących tzw. „rachunków uśpionych" z przepisami o ochronie danych osobowych.

Prezes UODO zwrócił uwagę, że przepisy wyżej wymienionych ustaw nakładają na banki i spółdzielcze kasy oszczędnościowo-kredytowe obowiązek przekazywania gminom szeregu informacji objętych tajemnicą bankową albo tajemnicą zawodową, w tym również danych osobowych, których przetwarzanie przez gminy nie znajduje uzasadnienia. Natomiast stwarza to

ryzyko nadmiarowego przetwarzania danych osobowych przez gminy. Obowiązek przekazywania przez banki i spółdzielcze kasy oszczędnościowo-kredytowe gminom informacji o posiadaczu rachunku (art. 111c ustawy Prawo bankowe i art. 13c ustawy o spółdzielczych kasach oszczędnościowo-kredytowych) dotyczy zarówno przypadku rozwiązania umowy rachunku z powodu śmierci posiadacza rachunku bankowego (śmierci członka spółdzielczej kasy oszczędnościowo-kredytowej posiadającego imienny rachunek), jak i wygaśnięcia umowy rachunku ze względu na długotrwały brak aktywności posiadacza tego rachunku. W przypadku rozwiązania umowy rachunku z powodu śmierci posiadacza albo członka spółdzielczej kasy oszczędnościowo-kredytowej, informowanie gminy i przekazywanie jej pewnych informacji przez banki i spółdzielcze kasy oszczędnościowo kredytowe, można uznać za uzasadnione, gdyż gmina może stać się spadkobiercą koniecznym takiego posiadacza na podstawie art. 935 zdanie pierwsze i art. 1023 § 1 Kodeks cywilny. W przypadku zaś wygaśnięcia umowy rachunku z powodu długotrwałego braku aktywności posiadacza rachunku albo członka spółdzielczej kasy oszczędnościowo-kredytowej, przekazywanie przez banki i spółdzielcze kasy oszczędnościowo-kredytowe gminie jakichkolwiek informacji o posiadaczu takiego rachunku nie jest prawidłowe, gdyż nie ma podstaw do stwierdzenia, że posiadacz rachunku (członek spółdzielczej kasy oszczędnościowo-kredytowej) zmarł, a zatem gmina nie jest w takiej sytuacji nawet potencjalnym spadkobiercą. W ocenie organu również zakres informacji udostępnianych gminie jest zbyt szeroki. O ile sama informacja o śmierci posiadacza rachunku (członka spółdzielczej kasy oszczędnościowo-kredytowej) może być gminie potrzebna do przeprowadzenia postępowania spadkowego, to brak jest podstaw, by informować gminę o dacie wydania przez posiadacza rachunku (członka spółdzielczej kasy oszczędnościowo-kredytowej) ostatniej dyspozycji dotyczącej tego rachunku, wysokości środków pieniężnych zgromadzonych na rachunku oraz kwotach i tytułach wypłat dokonanych z rachunku, a także źródle i podstawie dokonanych ustaleń. Poza tym ustawodawca nie dookreślił w przepisach, jaki okres wstecz powinna obejmować informacja o kwotach i tytułach wypłat dokonanych z rachunku.

Publikowanie na stronach Biuletynu Informacji Publicznej

Administrator, publikując dane osobowe na stronach BIP, powinien to robić w sposób dokładny i staranny. Powinien ponadto regularnie dokonywać przeglądu przetwarzanych zbiorów pod kątem usuwania zbędnych danych. Administrator odpowiedzialny za publikowanie treści w BIP jest zobowiązany do każdorazowego dokonania stosownej oceny, tak zasadności upublicznienia danych osobowych konkretnej osoby, jak i określenia okresu ich retencji. Podmioty

publiczne coraz częściej dokonują anonimizacji treści publikowanych w BIP, jednak nie robią tego w sposób kompleksowy, co świadczy o braku wiedzy na temat samej definicji danych osobowych. W ich ocenie tożsamość osoby jest możliwa do ustalenia jedynie na podstawie takich danych, jak imię i nazwisko. W jednej ze spraw[210] rozstrzygniętych przez Prezesa Urzędu, burmistrz w treści udostępnionej uchwały pozostawił niezanonimizowane takie dane, jak: nazwa miejscowości oraz numer posesji. Prezes Urzędu, działając na mocy art. 52 ust. 1 ustawy o ochronie danych osobowych[211], skierował do burmistrza wystąpienie zmierzające do zapewnienia skutecznej ochrony danych osobowych.

Pozyskiwanie szerokiego zakresu danych nabywców węglowych[212]

Prezes Urzędu Ochrony Danych Osobowych na podstawie art. 52 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[213] skierował do Ministra Finansów wystąpienie o dokonanie zmian w ***ustawie z dnia 6 grudnia 2008 r. o podatku akcyzowym***[214], celem dostosowania zawartych w niej regulacji, dotyczących pozyskiwania danych osobowych od finalnych nabywców węglowych, do zasad wyrażonych w ogólnym rozporządzeniu o ochronie danych. Prezes UODO wskazał, że obowiązujące od 1 stycznia 2019 r. przepisy powołanej ustawy, w tym jej art. 31a, prowadzą do nadmiarowego pozyskiwania danych. Tymczasem zgodnie z zasadą „minimalizacji danych" wyrażoną w art. 5 ust. 1 lit. c RODO, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. W przypadku sprzedaży węgla osobom fizycznym, sprzedawca pozyskuje od nabywcy takie dane, jak: imię i nazwisko, adres zamieszkania, numer dowodu osobistego lub nazwę i numer innego dokumentu stwierdzającego tożsamość oraz numer PESEL.

Minister Finansów pismem z dnia 16 września 2019 r. przekazał Prezesowi UODO do zaopiniowania projekt ***ustawy o zmianie ustawy o podatku akcyzowym oraz niektórych innych ustaw***, w którym został zawężony zakres przetwarzanych danych osobowych, co było przedmiotem wspomnianego wystąpienia Prezesa Urzędu Ochrony Danych Osobowych z 12.02.2019 r. skierowanego do Ministra Finansów. W projekcie ustawy przewidziano odstąpienie od wymogu podania numeru dowodu osobistego lub nazwy i numeru innego dokumentu stwierdzającego tożsamość; pozostawiono natomiast wymóg podania numeru PESEL, który pozwoli organom

[210] ZSPU.440.360.2019
[211] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[212] ZSPU.023.38.2019
[213] Dz. U. z 2018 r. poz. 1000 z późn. zm.
[214] Dz. U. z 2018 r. poz. 1114 z późn. zm.

podatkowym, przy ewentualnej kontroli, na właściwą identyfikację osób składających oświadczenie w zakresie wyrobów węglowych.

Ujawnianie numeru PESEL w podpisie elektronicznym i jawność numeru PESEL w Krajowym Rejestrze Sądowym

Upublicznianie numeru PESEL, który w Polsce jest krajowym numerem identyfikacyjnym, to dla Prezesa UODO niezwykle ważna kwestia. Zgodnie z obecnie obowiązującymi przepisami ujawnianie numeru PESEL w Krajowym Rejestrze Sądowym, a także w kwalifikowanym podpisie elektronicznym, jest dopuszczone ustawowo. Niemniej w opinii Prezesa UODO te przepisy, zapewniające legalność takiego przetwarzania danych, powinny być zmodyfikowane, gdyż wzbudzają wątpliwość pod kątem zgodności z art. 87 RODO. Zgodnie z powołanym przepisem państwo może określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego, ale wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie. Biorąc pod uwagę powyższe unormowania Prezes UODO 14 czerwca 2019 r. skierował do Ministra Cyfryzacji wystąpienie[215] o dokonanie zmian ustawowych dotyczących kwalifikowanego podpisu elektronicznego. Wskazał, że o ile zasadne jest użycie numeru PESEL w przypadku weryfikacji osoby wnioskującej o wydanie certyfikatu kwalifikowanego podpisu elektronicznego, o tyle wątpliwości budzi ujawnianie numeru PESEL innym osobom, jako konsekwencja użycia podpisu elektronicznego. Użycie kwalifikowanego podpisu elektronicznego jest często wymagane dla prostej czynności technicznej, takiej jak przesłanie korespondencji stronie (co organowi nadzorczemu sygnalizują chociażby pracownicy sądów administracyjnych). Prezes zwrócił uwagę, że przetwarzanie numeru PESEL bez zachowania odpowiednich zasad bezpieczeństwa stwarza szereg zagrożeń dla prywatności osoby fizycznej. Ujawniony w wielu miejscach ułatwia kradzież tożsamości, a także profilowanie osoby bez jej wiedzy i zgody. Organ nadzorczy zauważył, że rozwiązaniem sprzyjającym prawu do prywatności byłoby powszechniejsze stosowanie narzędzia, które przewiduje eIDAS oraz ustawa z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej, tj. pieczęci elektronicznej, w której oprócz nazwy podmiotu i jego danych weryfikacyjnych, takich jak numer NIP i numer REGON, zawarte są dane osób reprezentujących określoną jednostkę organizacyjną podmiotu, którego pieczęć dotyczy, ale bez danych o tak szczególnym charakterze, jakim jest numer PESEL. W odpowiedzi na powyższe wystąpienie organ nadzorczy 16 lipca 2019 r. otrzymał informację, iż

[215] ZSPU.023.97.2019

Ministerstwo Cyfryzacji deklaruje dokonanie przeglądu regulacji dotyczących identyfikatorów używanych w podpisie elektronicznym. Odbyły się też spotkania przedstawicieli Urzędu Ochrony Danych Osobowych z przedstawicielami Ministerstwa Cyfryzacji oraz centrami dostarczającymi podpisy elektroniczne.

Zmiany w ustawie o Krajowym Rejestrze Sądowym

Z kolei do Ministra Sprawiedliwości Prezes Urzędu Ochrony Danych Osobowych zwrócił się z wystąpieniem[216] o dokonanie zmian w ustawie z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym[217].

Artykuł 35 pkt 1 tej ustawy zakłada, że ilekroć do Krajowego Rejestru Sądowego wpisuje się osobę fizyczną, zamieszcza się tam nazwisko i imiona oraz identyfikator nadany w systemie ewidencji ludności (numer PESEL). Jednocześnie art. 8 powyższej ustawy zakłada jawność Krajowego Rejestru Sądowego i jego bezwarunkową powszechną dostępność. Prezes UODO w swym wystąpieniu wskazał na konieczność dokonania weryfikacji, funkcjonującej obecnie na gruncie Krajowego Rejestru Sądowego, koncepcji jawności bezwzględnej numeru PESEL. Rozumiejąc przesłanki, dla których numer PESEL funkcjonuje jako dana jawna (bezpieczeństwo obrotu gospodarczego) wskazał, że rozwiązania te zostały wprowadzone wiele lat temu, a konieczność przestrzegania przepisów RODO w polskim porządku prawnym sprzyja ponownej weryfikacji tej koncepcji. Każde podanie numeru PESEL do publicznej wiadomości dotyka również sfery prywatnej osoby. W przypadku Krajowego Rejestru Sądowego dotyczy to również osób, które nie sprawują już funkcji w podmiotach tam uwidocznionych, takich jak byli pełnomocnicy czy byli prokurenci. Numer PESEL osoby ujawniony w Krajowym Rejestrze Sądowym czyni go informacją powszechnie dostępną. Ministerstwo Sprawiedliwości w piśmie z 27 czerwca 2019 r. wskazało, że przetwarzanie danych osobowych, w tym numerów PESEL, w Krajowym Rejestrze Sądowym jest niezbędne do wykonania zadania realizowanego w interesie publicznym i jest proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

Niebieska Karta[218]

W związku z licznymi sygnałami ze strony urzędów miast i gmin, wyrażającymi wątpliwości co do zakresu danych osobowych, które mają prawo udostępniać osobom dotkniętym przemocą oraz osobom podejrzewanym o stosowanie przemocy w rodzinie, Prezes Urzędu Ochrony Danych

[216] ZSPU.023.53.2019
[217] Dz. U. z 2018 r. poz. 986 z późn. zm.
[218] ZSPU.023.152.2019

Osobowych zwrócił się do Ministra Rodziny, Pracy i Polityki Społecznej o wprowadzenie zmian przepisów normujących procedurę „Niebieskiej Karty".

Prezes UODO zwrócił uwagę, że 4 maja 2019 r., w związku z wejściem w życie ustawy z dnia 21 lutego 2019 o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych)[219], wprowadzono normę prawną, która w sposób znaczący ogranicza dostęp do danych osobowych przetwarzanych w toku procedury „Niebieskiej Karty". Dostęp do tych danych odbywa się na zasadzie wyłączeń, które są niejasne dla podmiotów stosujących te regulacje. W jednym ze wspomnianych wyłączeń pojawiło się określenie „innych dokumentów", co w konsekwencji prowadzi do tego, że ograniczenie prawa dostępu do danych osobowych nie następuje na poziomie prawa powszechnie obowiązującego, tylko jest zależne od uznania konkretnego urzędnika. Organ nadzorczy – mając na uwadze dobro i bezpieczeństwo ofiar przemocy – wskazał, że ograniczenia dostępu do danych powinny być wprowadzone rozważnie i ograniczone jedynie do tego, co niezbędnie konieczne. W odpowiedzi z 13 sierpnia 2019 r. Ministerstwo Rodziny, Pracy i Polityki Społecznej poinformowało, że zgłoszone uwagi organu nadzorczego będą przedmiotem analizy w kontekście ewentualnych zmian prawnych przepisów rozporządzenia Rady Ministrów z dnia 13 września 2011 r. w sprawie procedury „Niebieskiej Karty".

Program badań statystycznych statystyki publicznej[220]

W związku z sygnalizowanymi Prezesowi Urzędu Ochrony Danych Osobowych wątpliwościami pojawiającymi się w procesie pozyskiwania danych na potrzeby programu badań statystycznych statystyki publicznej na rok 2019, prowadzonego przez Główny Urząd Statystyczny (GUS), Prezes UODO swoimi spostrzeżeniami w tym zakresie podzielił się z Prezesem GUS, wyrażając troskę o zapewnienie odpowiedniej ochrony danych osobowych przetwarzanych na potrzeby realizacji powyższego programu.

Wskazał przy tym, że z informacji uzyskanych od instytucji publicznych, przede wszystkim gmin, wynika, że podmioty te mają wątpliwości, czy mogą pozyskiwać i przekazywać GUS dane od podległych im jednostek w związku z realizacją programu badań statystycznych statystyki

[219] Dz. U. poz. 730
[220] ZSPU.070.9.2019

publicznej. W ocenie Prezesa UODO, o ile zrozumiałe jest, że GUS może realizować swoje uprawnienia, wnioskując bezpośrednio do jednostek będących w posiadaniu danych o ich przekazanie w zakresie wynikającym z przepisów o statystyce publicznej, o tyle wątpliwości budzi żądanie pozyskania danych osobowych przez jednostki wyższego rzędu od jednostek im podległych celem przekazania ich do GUS. Natomiast w przypadku podmiotów z sektora prywatnego podnoszone jest m.in. to, że nie zawsze znajdują się one w posiadaniu wnioskowanych przez GUS danych, a z przepisów prawa nie wynika, aby miały prawo do ich pozyskania i dalszego przetwarzania. Przykładem jest sytuacja, gdy przedsiębiorca dysponuje adresem, pod którym świadczona jest usługa, ale nie posiada adresu zamieszkania usługodawcy, o który pyta GUS. Organ ochrony danych osobowych podkreślił, że ważne jest m.in. to, by wniosek o przekazanie danych był skierowany do podmiotów, które są ich administratorami, i by istniała podstawa uprawniająca do żądania udostępnienia danych. Z kolei podmioty, które miałyby udostępniać dane osobowe muszą pamiętać o przestrzeganiu przepisów o ochronie danych osobowych i – zgodnie z wynikającą z RODO zasadą rozliczalności – być w stanie to wykazać. Przepisy z zakresu statystyki publicznej są podstawą do udostępnienia jedynie tych danych osobowych, które administrator może posiadać zgodnie z prawem dla realizacji ściśle określonych celów, przy zachowaniu zasad, o których mowa w art. 5 RODO, w tym zasady proporcjonalności, minimalizacji i ograniczenia czasowego. W odpowiedzi na to wystąpienie Prezes GUS nadesłał obszerne wyjaśnienia odnoszące się do wszystkich sygnalizowanych zagadnień. Wskazał w nim m.in., że do gmin przesłane zostało pismo informujące, o przekazanie jakich danych GUS prosi. Podkreślił też, że „w celu bezpiecznego transferu danych został udostępniony system teleinformatyczny (TransGUS), z użyciem szyfrowanego połączenia i dedykowanego systemu uprawnień". Odnosząc się do uwag dotyczących pozyskiwania danych z rejestrów prowadzonych przez operatorów publicznie dostępnych usług telekomunikacyjnych, Prezes GUS zapewnił, że „nie było intencją GUS poszerzanie zakresu danych osobowych zbieranych i przetwarzanych przez operatorów publicznie dostępnych usług telekomunikacyjnych, wyłącznie dla realizacji zadań GUS. W związku z tym operatorzy usług telekomunikacyjnych będą poproszeni o przekazanie tych danych z katalogu wymienionego w aktach prawnych, które znajdują się w ich zasobach informacyjnych". Prezes GUS zapewnił jednocześnie, że wątpliwości zgłoszone przez Prezesa UODO „zostaną potraktowane jako postulaty *de lege ferenda* w odniesieniu do Programów na kolejne lata, m.in. w kwestii takiego sformułowania zapisów Programu, który nie będzie budził zastrzeżeń, co do podmiotów uprawnionych do przekazywania danych".

Wykonywanie kopii dokumentów[221]

W 2019 r. Prezes Urzędu Ochrony Danych Osobowych wystąpił do Ministra Rodziny, Pracy i Polityki Społecznej o dokonanie zmian w rozporządzeniu Ministra Rodziny, Pracy i Polityki Społecznej z dnia 7 grudnia 2017 r. w sprawie wydawania zezwolenia na pracę cudzoziemca oraz wpisu oświadczenia o powierzeniu wykonywania pracy cudzoziemcowi do ewidencji oświadczeń[222].

Podmioty powierzające wykonywanie pracy cudzoziemcowi mają obowiązek dołączania do wniosków o wydanie zezwolenia na pracę oryginału ważnego dowodu osobistego. Rozporządzenie uprawnia podmiot powierzający pracę cudzoziemcowi do dołączania kopii ważnego dowodu osobistego do wniosku w miejsce oryginału (jeżeli oryginał zostanie przedstawiony do wglądu pracownikowi organu prowadzącemu postępowanie). Biorąc pod uwagę fakt, że dowód osobisty jest dokumentem tak istotnym dla osoby nim się legitymującej, w większości przypadków będzie dochodzić do dołączenia jego kopii w miejsce oryginału i tym samym pozyskiwania przez organ prowadzący postępowanie kopii dowodu osobistego. Dowód osobisty służy przede wszystkim potwierdzeniu tożsamości osoby fizycznej i obywatelstwa z funkcją umożliwienia przekraczania granic państw; jest też nośnikiem wielu różnych danych osobowych. Organ nadzorczy wskazał, że zgodnie z zasadą minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c RODO, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Ograniczenie do danych niezbędnych oznacza takie ukształtowanie zakresu przetwarzania danych, aby były pozyskiwane i wykorzystywane tylko te dane, które są niezbędne do osiągnięcia zamierzonego celu przetwarzania tak, aby nie ingerować nadmiernie w prawo do prywatności osoby fizycznej. Administrator powinien pozyskiwać dane jedynie w niezbędnym i prawnie uzasadnionym zakresie. Zabronione jest przy tym pozyskiwanie danych osobowych na zapas. Prezes UODO podkreślił, że przy składaniu wniosków drogą elektroniczną, składanie dokumentów odbywa się przy jednoczesnym uwierzytelnieniu tożsamości za pomocą takich narzędzi, jak kwalifikowany podpis elektroniczny czy podpis potwierdzony profilem zaufanym ePUAP. W związku z tym dodatkowe potwierdzenie tożsamości przy pomocy kopii ważnego dowodu osobistego jest niecelowe oraz nadmiarowe. W odpowiedzi[223] na to wystąpienie z 20 lutego 2019 r. w sprawie zmiany przepisów w sprawie wydawania zezwolenia na pracę cudzoziemca, Ministerstwo Rodziny, Pracy i Polityki Społecznej wskazało, że ze względu na przedstawione

[221] ZSPU.027.67.2019
[222] Dz. U. z 2017 r. poz. 1265
[223] Pismo z 2 kwietnia 2019 r. sygn. DRP.VIII.40320.4.1.2019.MP.

argumenty, wskazujące, iż ten sposób potwierdzenia tożsamości jest sprzeczny z zasadami wynikającymi z RODO, podjęte zostały prace mające na celu ustalenie innych sposobów potwierdzenia tożsamości podmiotu powierzającego wykonywanie pracy cudzoziemcowi, które będą mogły wiązać się ze zniesieniem wymogu dołączania kopii dowodu osobistego do wniosku lub oświadczenia.

Kserokopie dowodów osobistych[224]

W 2019 r. Prezes Urzędu Ochrony Danych Osobowych skierował do Ministra Spraw Wewnętrznych i Administracji wystąpienie o podjęcie prac legislacyjnych mających na celu uregulowanie w przepisach prawa ograniczeń w zakresie sporządzania kserokopii dowodów osobistych oraz stworzenie narzędzi prawnych pomocnych w zwalczaniu zjawiska tzw. kradzieży tożsamości. Organ nadzorczy postulował, by dokonano przeglądu regulacji stanowiących podstawę prawną do sporządzania replik dowodów tożsamości, a następnie o podjęcie prac legislacyjnych tak, by zgodnie z zasadą minimalizacji danych, możliwość sporządzania replik ograniczyć w przepisach jedynie do sytuacji, gdy jest to niezbędne. Rozwiązaniem rekomendowanym przez organ nadzorczy było dodatkowo zawarcie w ustawie o dokumentach publicznych przepisów doprecyzowujących w sposób szczegółowy, w jakich sytuacjach sporządzenie replik dokumentów publicznych jest dopuszczalne, co pozwoliłoby jednoznacznie ocenić, czy dokonanie tej czynności jest niezbędne, np. w postaci zamkniętego katalogu przesłanek dających podstawę do wykonania repliki. Innym rozwiązaniem zwiększającym bezpieczeństwo obrotu replikami dowodów tożsamości, w kontekście zagrożeń związanych z kradzieżami tożsamości, może być wprowadzenie do przepisów ustawy o dokumentach publicznych obligatoryjnego obowiązku oznaczania takich replik niezwłocznie po ich wykonaniu – i to w taki sposób, by jednoznacznie odróżniały się od kopiowanego dokumentu tożsamości. W ocenie Prezesa Urzędu Ochrony Danych Osobowych, w przypadku wprowadzenia obowiązku oznaczania wykonanych replik dokumentu tożsamości, ustawodawca powinien również dokonać penalizacji braku wykonania takiego obowiązku przez osobę sporządzającą replikę. W opinii organu nadzorczego wskazana inicjatywa ustawodawcza powinna być poprzedzona dokonaniem w Ministerstwie Spraw Wewnętrznych i Administracji przeglądu regulacji stanowiących podstawę prawną do sporządzania replik dowodów tożsamości, tak by projekt nowelizacji ustawy o dokumentach publicznych ograniczał możliwość legalnego sporządzania replik jedynie do sytuacji, gdy jest to niezbędne. Dodatkowo istotnym mechanizmem,

[224] ZSPU.023.87.2018

który znacznie zwiększyłby bezpieczeństwo przy sporządzaniu replik dokumentów publicznych (w tym sporządzanie kserokopii dowodów osobistych), byłoby nałożenie obowiązku oznaczania replik niezwłocznie po wykonaniu, tak by jednoznacznie odróżniały się od kopiowanego dokumentu. Istotnym elementem nowelizacji ustawy o dokumentach publicznych, o którą wnioskował organ nadzorczy, powinno być również zawarcie w jej przepisach podstaw prawnych do stworzenia państwowego elektronicznego systemu umożliwiającego zgłaszanie utraty dokumentów tożsamości przez obywateli.

Ostatecznie resort przygotował nową ustawę o dokumentach publicznych, która weszła w życie 12 lipca 2019 r. W opinii organu ds. ochrony danych osobowych, choć nie rozwiązuje ona wszystkich problemów, powinna przyczynić się do poprawy bezpieczeństwa danych osobowych i utrudnić wykorzystanie kopii dokumentów do kradzieży tożsamości.

Przetwarzanie danych osobowych byłych pracowników

W 2019 r. Prezes UODO wydał na podstawie art. 52 ust. 1 ustawy z 2018 r. dwa wystąpienia skierowane do będącej podmiotem leczniczym spółki jawnej[225].

Impulsem do skierowania wystąpień była informacja w związku z postępowaniem administracyjnym toczącym się na skutek złożonych skarg na nieprawidłowości w procesie przetwarzania przez ww. spółkę danych osobowych byłych pracowników. Nieprawidłowości te polegały na wykorzystaniu przez wspólnika spółki jawnej danych osobowych byłych pracowników, przetwarzanych przez spółkę w związku ze stosunkiem pracy, do uzyskania nieuprawnionego dostępu do danych tych pracowników (w tym danych dotyczących stanu zdrowia), za pośrednictwem Platformy Usług Elektronicznych Zakładu Ubezpieczeń Społecznych. Wspólnik spółki wykorzystał dane osobowe byłych pracowników w zakresie ich numerów PESEL, znajdujących się w prowadzonej przez spółkę dokumentacji pracowniczej, do uzyskania dostępu do danych osobowych za pośrednictwem Platformy Usług Elektronicznych Zakładu Ubezpieczeń Społecznych w celach szkoleniowych, na potrzeby doskonalenia umiejętności wystawiania elektronicznych zwolnień lekarskich. Wykorzystanie danych osobowych przez wspólnika nastąpiło zatem w celu innym, niż ten, dla którego zostały one zebrane. Wspólnik ww. spółki uzyskał ponadto dostęp do danych osobowych byłych pracowników za pośrednictwem Platformy Usług Elektronicznych Zakładu Ubezpieczeń Społecznych, w związku z wykonywanym zawodem

[225] ZSZZS.440.217.2018, ZSZZS.440.218.2018.

lekarza, pomimo iż osoby te nie były jego pacjentami, powyższe nastąpiło więc bez podstawy prawnej.

Prezes UODO wskazał, że na podstawie art. 5 ust. 1 RODO dane osobowe muszą być przetwarzane m.in. zgodnie z prawem, zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane oraz przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem za pomocą odpowiednich środków technicznych lub organizacyjnych. Natomiast administrator na podstawie art. 5 ust. 2 RODO odpowiada za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie. Prezes UODO zaznaczył, że rozwinięciem określonej w art. 5 ust. 1 lit f zasady bezpieczeństwa danych osobowych są przepisy art. 24 i 32 RODO. Zgodnie z art. 24 ust. 1 administrator – uwzględniając charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw lub wolności osób fizycznych – wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Z kolei na podstawie art. 32 ust. 1 RODO wdraża on odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym m.in. w stosownym przypadku: pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania. Właściwe zabezpieczanie danych osobowych ma prowadzić do braku naruszeń (lub ich minimalizacji) w kontekście m.in. nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 pkt 12 RODO). Obowiązkiem każdego pracodawcy jest chronić dane osobowe pracowników przed ich przetwarzaniem w sposób niezgodny z prawem. Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Prezes podniósł, że obowiązkiem spółki było zapewnienie, aby dane pracowników (w tym numer PESEL) zawarte w dokumentacji pracowniczej prowadzonej przez spółkę, przetwarzane były w celu, dla którego zostały pozyskane, tj. w celu realizacji praw i obowiązków związanych z łączącym ww. osoby i spółkę stosunkiem pracy.

Odnosząc się natomiast do nieuprawnionego uzyskania przez wspólnika spółki, przy użyciu numerów PESEL byłych pracowników, dostępu do innych danych osobowych tych osób za pośrednictwem Platformy Usług Elektronicznych Zakładu Ubezpieczeń Społecznych w celach szkoleniowych, na potrzeby doskonalenia umiejętności wystawiania elektronicznych zwolnień

lekarskich, Prezes UODO wskazał, że w obecnym stanie prawnym brak jest przepisów, które legalizowałyby pozyskiwanie przez lekarzy dostępu do danych osobowych za pośrednictwem ww. Platformy w celu innym niż wystawienie, anulowanie lub sprostowanie zaświadczenia lekarskiego. Organ zaznaczył, że dane osobowe udostępniane wystawiającym zaświadczenie lekarskie w ww. Platformie dotyczą między innymi stanu zdrowia pacjentów, a zatem danych, które podlegają szczególnej ochronie.

Prezes UODO wskazał, że zgodnie z art. 6 ust. 4 RODO, jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: a) wszelkie związki między celami, w których zebrano dane osobowe a celami zamierzonego dalszego przetwarzania; b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10; d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji. Z art. 13 ust. 3 RODO wynika zaś, że jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich stosownych informacji. Z tych samych względów niedopuszczalne jest, w ocenie Prezesa UODO, przetwarzanie danych osobowych pracownika bez wyraźnej podstawy prawnej lub udzielonej przez tego pracownika zgody. Takie działanie jest naruszeniem zasad bezpieczeństwa.

III. DZIAŁALNOŚĆ EDUKACYJNO - INFORMACYJNA

Zgodnie z treścią art. 57 RODO, podstawowe zadania edukacyjno–informacyjne 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*[226];
- *upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO*[227];
- *udzielanie osobie, której dane dotyczą, na jej żądanie, informacji o wykonywaniu praw przysługujących jej na mocy RODO, a w stosownym przypadku współpraca w tym celu z organami nadzorczymi innych państw członkowskich*[228].

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

W ramach prowadzonej działalności edukacyjnej w 2019 roku organ właściwy w sprawie 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. Tematyka szkoleń przeprowadzonych przez przedstawicieli Urzędu dla kadry zarządzającej i pracowników różnych instytucji i organizacji, głównie dotyczyła zagadnień związanych z RODO. Tematem były nowe przepisy o ochronie danych osobowych w praktyce organów administracji publicznej i innych podmiotów.

W sumie w 2019 r. przeprowadzono **25 szkoleń podmiotów zewnętrznych** (zał. 1).

Wśród podmiotów, które w 2019 r. zwróciły się do Urzędu Ochrony Danych Osobowych z prośbą o przeprowadzenie szkolenia znalazły się: kadra zarządzająca MSWiA, wojewodowie i dyrektorzy Urzędów Wojewódzkich oraz Inspektorzy Ochrony Danych Osobowych działający w Urzędach Wojewódzkich z całej Polski, sędziowie Krajowej Rady Sądownictwa, kadra

[226] Art. 57.1.b RODO
[227] Art. 57.1.d RODO
[228] Art. 57.1.e RODO

zarządzająca i pracownicy Centrali KRUS, przedstawiciele regionalnych dyrekcji ochrony środowiska, IOD Komendy Głównej Policji oraz Kancelaria Prezesa Rady Ministrów w ramach VII Dnia Otwartego dla służby cywilnej. Przedstawiciele UODO przeprowadzili także szkolenia dla kadry zarządzającej i pracowników Biura Komisji Sejmowych, Wydziału Edycji Tekstów z Posiedzeń Komisji oraz Ośrodka Informatyki Kancelarii Sejmu RP. Szkolenie to obejmowało swoim zakresem problematykę ochrony danych osób fizycznych, które wypowiadają się w toku posiedzeń komisji i podkomisji sejmowych oraz osób, o których może być mowa w trakcie takich posiedzeń, a także możliwe sposoby ich anonimizacji w pełnych zapisach z przebiegu tych posiedzeń. Dodatkowym zagadnieniem była anonimizacja odpowiednich fragmentów transmisji z przebiegu posiedzeń komisji i podkomisji zamieszczanych w Systemie Informacyjnym Sejmu.

Na uwagę zasługuje także odprawa szkoleniowa w MSWiA dla Inspektorów Ochrony Danych (11.04.2019 r.) powołanych na poziomie jednostek centralnych oraz wojewódzkich w służbach nadzorowanych przez ministra właściwego do spraw wewnętrznych, podczas której przedstawiciele Urzędu przeprowadzili szkolenie z zakresu ochrony danych osobowych. W trakcie tej całodniowej odprawy dokonane zostało podsumowanie działań Biura Nadzoru Wewnętrznego MSWiA w zakresie analizy i oceny przetwarzania danych osobowych przez Policję, Straż Graniczną, Służbę Ochrony Państwa i Państwową Straż Pożarną oraz ujawnianie nieprawidłowości w tym zakresie.

Niektóre szkolenia miały **cykliczny charakter**, jak szkolenie realizowane w ramach X edycji ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", które odbyło się w dniach 2-3 października 2019 r. w Senacie RP. Inne zaś dodatkowo odbywały się w formule wirtualnej, jak szkolenia podmiotów sektora publicznego w ramach projektu **T4DATA,** współfinansowanego ze środków Unii Europejskiej z Programu „Prawa, Równość i Obywatelstwo (2016-2020)". W ramach projektu T4DATA uruchomiona została specjalna platforma z wykładami online[229], dzięki której inspektorzy ochrony danych w podmiotach publicznych zyskali dodatkową możliwość uzupełnienia wiedzy na temat prawidłowego stosowania ogólnego rozporządzenia o ochronie danych. Użytkownicy platformy dodatkowo mogli obejrzeć wykłady zarejestrowane podczas szkoleń lokalnych dla IOD, które UODO zorganizował na przełomie maja i czerwca 2019 r. w Poznaniu, Gdyni, Rzeszowie i Warszawie.

W formule **szkoleń online (webinariów) dla sektora oświaty** Urząd Ochrony Danych Osobowych – przy współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów

[229] https://t4data.uodo.gov.pl/

w Warszawie – transmitował wykłady dla uczniów i nauczycieli, poświęcone następującym zagadnieniom:

- monitoring wizyjny w szkole – aspekty prawne i techniczne,
- obowiązek informacyjny w szkole,
- zasady ochrony danych osobowych przy rekrutacji do szkół,
- przetwarzanie danych przy organizacji szkolnych konkursów,
- zasady prowadzenia dokumentacji psychologiczno-pedagogicznej,
- przetwarzanie danych uczniów w celu realizacji praktyk lub stażu,
- prowadzenie przez szkoły rejestru czynności przetwarzania.

W celu propagowania wiedzy o ochronie danych osobowych prowadzony jest serwis informacyjny **techinfo.uodo.gov.pl**[230], poświęcony m.in. tematyce wykorzystywania danych osobowych w związku z rozwojem nowoczesnych technologii, organizowanym przez UODO konferencjom, seminariom i szkoleniom. Portal oferuje również dostęp do poradników dotyczących ochrony danych osobowych.

Szkolenia sektorowe Inspektorów Ochrony Danych

W 2019 r. organ właściwy do spraw ochrony danych kontynuował – zainicjowany w 2016 r. – cykl nieodpłatnych szkoleń dla inspektorów ochrony danych (IOD) wybranych sektorów.

Od 2016 r. odbyło się 16 ww. szkoleń, z czego pięć w 2018 r. oraz **cztery w 2019 r.**

1. Szkolenie pt. „Zgłaszanie naruszenia ochrony danych osobowych" (14.01.2019 r.).
2. Szkolenie pt. „Zasady przetwarzania danych w świetle ustawy wdrażającej dyrektywę 2016/680" (12.02.2019 r.).
3. Szkolenie pt. „Przekazywanie danych do państw trzecich" (20.02.2019 r.).
4. Szkolenie pt. „Obowiązek informacyjny" (28.02.2019 r.).

Sektorowe szkolenia koncentrowały się na nowych unijnych przepisach o ochronie danych osobowych oraz przepisach krajowych, mających zastosowanie do przetwarzania danych w określonej dziedzinie działalności.

Ogółem w szkoleniach IOD organizowanych przez Urząd wzięło udział ponad 8000 uczestników. Szkolenia te transmitowane były na żywo, a następnie udostępniane na kanale YouTube, osiągając liczbę prawie 20 tys. wyświetleń[231]. Dla przykładu, szkolenie dla IOD-ów dot. „Zgłaszania naruszenia ochrony danych osobowych" zostało odtworzone 3 037 razy;

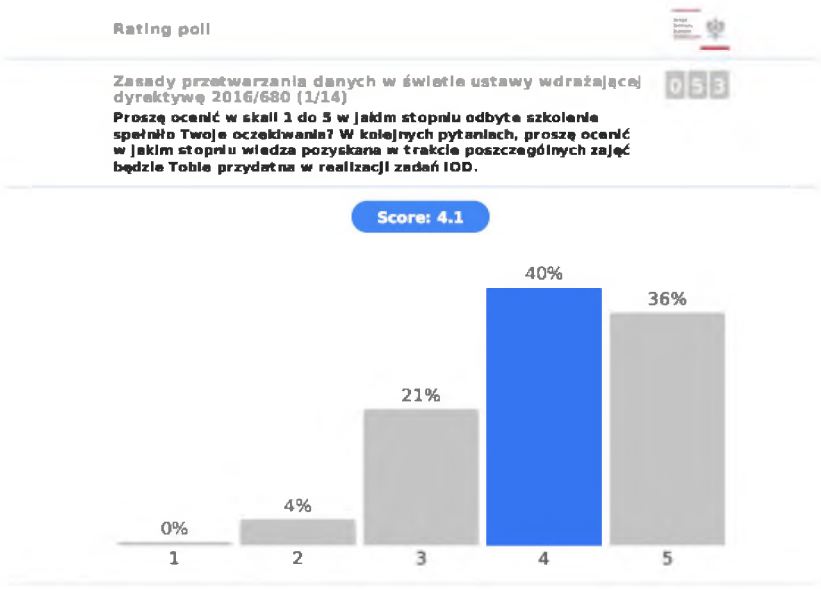
[230] https://techinfo.uodo.gov.pl
[231] Dane ze stycznia 2020 r.

„Przekazywanie danych do państw trzecich" – 2 789 razy; „Obowiązek informacyjny" – 11 071 razy. Treści prezentowane podczas szkoleń są dostępne na stronie internetowej organu ds. ochrony danych.

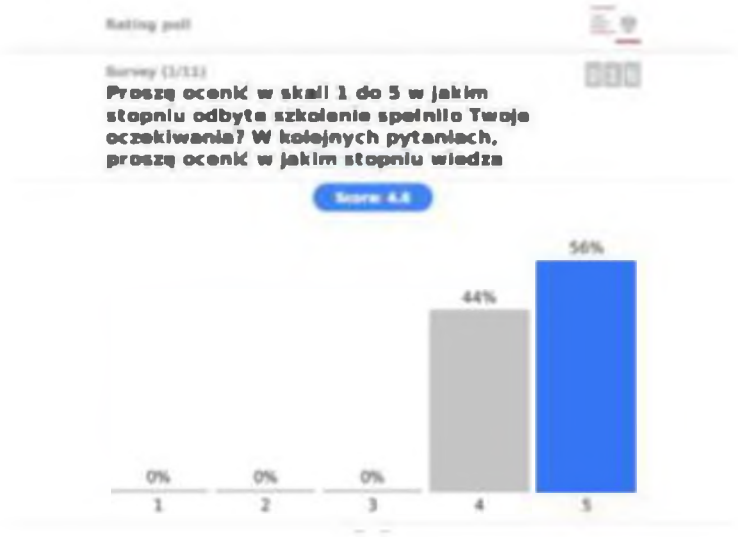
Szkolenia te nie tylko podniosły poziom wiedzy Inspektorów Ochrony Danych obsługujących daną branżę, ale stanowiły także okazję do wymiany doświadczeń, rozwiązań i dobrych praktyk pomiędzy uczestnikami tych spotkań.

Po przeprowadzonych szkoleniach do ich uczestników wysłana została ankieta ewaluacyjna z prośbą o ocenę. Poziom oczekiwań i satysfakcji respondentów w odniesieniu do poszczególnych szkoleń przeprowadzonych w 2019 roku przedstawiają poniższe wykresy, według podanej niżej skali:

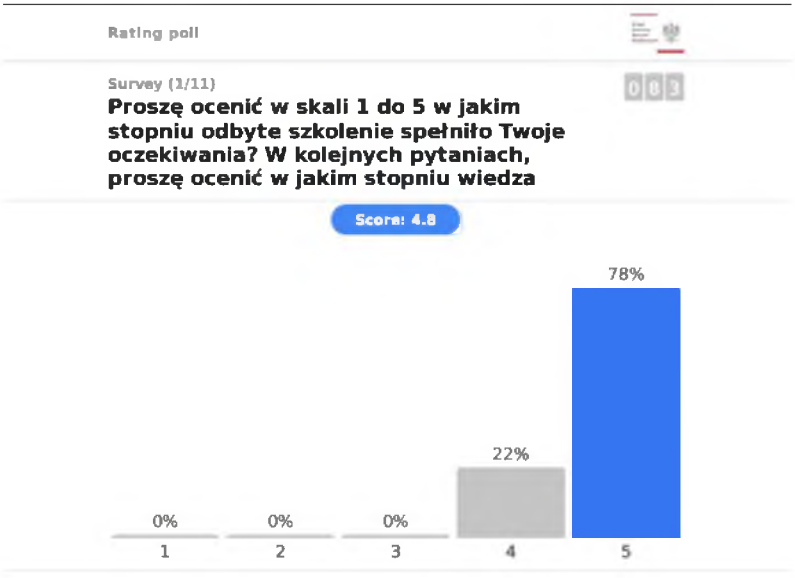
5 – bardzo dobrze
4 – dobrze
3 – średnio
2 – wystarczająco
1 – niewystarczająco



Wykres 9: Szkolenie „Zasady przetwarzania danych w świetle ustawy wdrażającej dyrektywę 2016/680" (12.02.2019).



Wykres 10: Szkolenie „Przekazywanie danych do państw trzecich" (20.02.2019) – ocena przez osoby uczestniczące w szkoleniu on-line.



Wykres 11: Szkolenie „Przekazywanie danych do państw trzecich" (20.02.2019) – ocena przez osoby bezpośrednio uczestniczące w szkoleniu.

Wykres 12: Szkolenie „Obowiązek informacyjny" (28.02.2019).

Szkolenia dla jednostek samorządu terytorialnego (JST)

W analizowanym okresie sprawozdawczym przedstawiciele organu nadzorczego kontynuowali zapoczątkowane w czerwcu 2018 roku szkolenia dla przedstawicieli jednostek samorządu terytorialnego. Odbywały się one pod nazwą: „Zmiany w zakresie ochrony danych osobowych w świetle RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych". Szkolenia te zorganizowane były we współpracy z Narodowym Instytutem Samorządu Terytorialnego (NIST) w 3 miastach wojewódzkich: w Łodzi (7.02.2019), Toruniu (8.02.2019) oraz Olsztynie (6.03.2019). Adresatami tych szkoleń byli pracownicy odpowiedzialni za bezpieczeństwo danych osobowych w jednostkach samorządu terytorialnego (starostw powiatowych, urzędów marszałkowskich, miast i gmin). Łącznie w tych 3 szkoleniach udział wzięło ponad 250 przedstawicieli jednostek samorządu terytorialnego.

Pomocny w podniesieniu wiedzy na temat nowego prawa w zakresie ochrony danych osobowych był również kurs e-learningowy „Zmiany w zakresie ochrony danych osobowych w świetle RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych" opracowany przez NIST przy merytorycznym wsparciu UODO. Kurs ten jest dostępny pod adresem: https://e-szkolenia.nist.gov.pl/ i kończy się egzaminem na platformie e-learningowej.

Podsumowując, w okresie niespełna 10 miesięcy (czerwiec 2018 r. – marzec 2019 r.) współorganizowane przez UODO i NIST szkolenia odbyły się w dwunastu miastach wojewódzkich. Łącznie wzięło w nich udział 1084 uczestników z 554 jednostek samorządu terytorialnego.

1.2. Konkursy

W analizowanym 2019 roku 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 IX edycji konkursu dla studentów prawa i administracji na esej dotyczący zagadnień z zakresu ochrony danych osobowych. Partnerem merytorycznym konkursu została Kobylańska & Lewoszewski Kancelaria Prawna sp. j. s.

Zadaniem konkursowym była ocena, czy w opisanym kazusie uczelnia X prawidłowo udostępniła dane osobowe studenta w świetle przepisów ogólnego rozporządzenia o ochronie danych. Autorzy nadesłanych prac wykazali się dużą wiedzą dotyczącą znajomości przepisów RODO oraz ustawy o ochronie danych osobowych. Swoje sądy oraz argumentację popierali literaturą przedmiotu, orzecznictwem sądowym, a także decyzjami Prezesa Urzędu Ochrony

Danych Osobowych. Organizowany cyklicznie konkurs miał na celu propagowanie wśród studentów polskich uczelni wiedzy z zakresu ochrony danych osobowych, umożliwienie im sprawdzenia swojej wiedzy w tej dziedzinie prawa, a także promowanie studentów posiadających umiejętność formułowania praktycznych rozwiązań w zetknięciu z problemami prawnymi.

Laureaci konkursu otrzymali nagrody rzeczowe oraz nagrody specjalne w postaci nieodpłatnych praktyk w Urzędzie Ochrony Danych Osobowych.

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

Już po raz siódmy zorganizowany został ogólnopolski konkurs dla szkół i ośrodków doskonalenia nauczycieli w ramach Programu „Twoje dane – Twoja sprawa", mający na celu promocję najciekawszej inicjatywy dotyczącej tematyki ochrony danych osobowych. Do konkursu zgłoszonych zostało **12 inicjatyw**. Przedmiotem oceny w ramach konkursu były działania podjęte przez uczestników programu oraz partnerów metodycznych, które wyróżniały się pomysłowością i wysokim poziomem merytorycznym przygotowanych materiałów, szerokim zasięgiem i efektywnością oddziaływania. I miejscem uhonorowany został projekt „Roduś w cyberprzestrzeni", za który **Szkoła Podstawowa nr 10 im. Księżnej Aleksandry Ogińskiej w Siedlcach** otrzymała szczególne wyróżnienie Prezesa Urzędu Ochrony Danych Osobowych – statuetkę „Złotego Pióra". Kolejni laureaci konkursu to: **Szkoła Podstawowa nr 360 w Warszawie** za inicjatywę pod nazwą „Udany Oficjalny Debiut Oryginalny – nasze wybory" (II miejsce)**, Szkoła Podstawowa nr 11 Specjalna. Specjalny Ośrodek Szkolno-Wychowawczy w Zamościu** (III miejsce) za inicjatywę „Dzień Ochrony Danych Osobowych – gra na korytarzu szkolnym. Nie daj się złapać w sieci".

3) Konkurs plastyczno-literacki dla uczniów

W ramach IX edycji programu TDTS, Prezes UODO zorganizował konkurs plastyczno-literacki dla uczniów pod nazwą **„(NIE) bezpieczne dane osobowe"**. Zadaniem konkursowym było przygotowanie pracy plastycznej lub opowiadania. Ze względu na dobre przygotowanie uczniów, ich wiedzę i twórcze podejście do tematu, wybór najlepszych spośród 103 (23 opowiadania i 82 prace plastyczne) nadesłanych prac był wyjątkowo trudny. W konkursie dla uczniów brana była pod uwagę innowacyjność pracy, wykorzystanie nowych i niestandardowych form wyrazu, a także jakość merytoryczna. Zwracano uwagę na rzetelne i dostosowane do wieku odbiorców przedstawienie kwestii ochrony prywatności. Komisja konkursowa wybrała trzy najlepsze prace oraz wyróżniła pięć. Laureatami konkursu plastyczno-literackiego zostali uczniowie

z następujących szkół: **Szkoły** z **Podstawowej nr 11 Specjalnej. Specjalny Ośrodek Szkolno-Wychowawczy w Zamościu** (I miejsce), **Szkoły Podstawowej im. Janka Bytnara „Rudego" w Lubieniu Kujawskim** (II miejsce), **Zespołu Szkół nr 3 im. 2 Armii Wojska Polskiego w Warszawie** (III miejsce). Wszystkie nagrodzone i wyróżnione prace konkursowe można oglądać na stronie internetowej Prezesa Urzędu[232].

1.3. Projekty i programy

W roku sprawozdawczym 2019, Urząd Ochrony Danych Osobowych kontynuował swój udział w różnego rodzaju projektach. Wśród nich wymienić należy projekt „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. oraz „T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych" – od stycznia 2018 r. Programy te finansowane są ze środków Komisji Europejskiej.

Ponadto w 2019 r. kontynuowany był krajowy program edukacyjny „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", który od 2009 r. nieprzerwanie realizowany jest przez Urząd Ochrony Danych Osobowych pod patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.

1) 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"

Realizacja projektu rozpoczęła się we wrześniu 2017 r. i trwała 2 lata. Projekt ten finansowany był ze środków Komisji Europejskiej w ramach programu Erasmus+ „Akcja 2 – Współpraca na rzecz innowacji i wymiany dobrych praktyk, Działanie – Partnerstwo strategiczne na rzecz edukacji osób dorosłych". Koordynatorem projektu była Komisja Ochrony Danych Osobowych w Bułgarii (CPDP), a partnerami: Urząd Ochrony Danych Osobowych, Chorwacka Agencja Ochrony Danych Osobowych (AZOP), Uniwersytet Sofijski im. św. Klemensa z Ochrydy, Uniwersytet Jagielloński oraz Włoska organizacja pozarządowa (GVMAS ONLUS).

[232] www.uodo.gov.pl/tdts

Celem międzynarodowego projektu „e-OpenSpace" było zagospodarowanie elektronicznej przestrzeni w formie **platformy e-learningowej**, złożonej z dwóch części: publicznej i prywatnej. Platforma ma za zadanie ułatwić obywatelom dostosowanie się do nowego systemu prawnego dotyczącego ochrony danych osobowych. W skład materiałów edukacyjnych nowo powstałej platformy będą wchodziły m.in. nagrania prezentacji, dokumenty, sekcja pytań i odpowiedzi.

Projekt zakończył się w sierpniu 2019 r. Ostatnie spotkanie partnerów projektu „e-OpenSpace" odbyło się **20 sierpnia 2019 r.** w siedzibie polskiego organu właściwego do spraw ochrony danych osobowych. Jego celem była dyskusja na temat działań promocyjnych dotyczących platformy, a także podsumowanie dotychczasowych działań. Koordynator projektu – przedstawiciel bułgarskiej Komisji Ochrony Danych Osobowych (CPDP) – potwierdził, że założenia projektu zostały całkowicie zrealizowane. Zakończyły się prace związane z technicznymi aspektami uruchomienia platformy e-learningowej, w szczególności nad oferowanymi wersjami językowymi tego narzędzia: angielską, bułgarską, chorwacką, polską oraz włoską. Użytkownicy platformy będą mogli m.in. skorzystać z 10 kursów przedstawiających zarówno ogólne, jak i bardziej szczegółowe zagadnienia z zakresu ogólnego rozporządzenia o ochronie danych. W założeniu platforma e-learningowa ma być bazą informacji dostępnych dla wszystkich, którzy chcieliby zarówno rozpocząć naukę o ochronie danych osobowych, pogłębić oraz ugruntować posiadaną już wiedzę z tego zakresu, zaś osobom nauczającym o RODO – umożliwi tworzenie autorskich programów szkoleniowych.

2) T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych

„T4DATA" to międzynarodowy projekt, którego celem jest wsparcie organów nadzorczych oraz IOD podmiotów publicznych, na rzecz szkoleń w zakresie nowego prawa o ochronie danych osobowych. Celem projektu było wypracowanie jednolitego rozumienia i interpretacji wymogów RODO, a w konsekwencji wzmocnienie wzajemnego zaufania między organami ochrony danych w zakresie stosowania nowego prawa o ochronie danych osobowych. Ogólne rozporządzenie o ochronie danych nakłada bowiem na administratorów wiele nowych obowiązków – na czele z zupełnie nowym podejściem do ochrony danych osobowych wyrażonym w zasadzie rozliczalności. Urząd Ochrony Danych Osobowych rozpoczął realizację dwuletniego projektu „T4DATA" w styczniu 2018 r., podczas którego wspólnie z organami ochrony danych z Włoch, Hiszpanii, Bułgarii i Chorwacji przygotowany został cykl szkoleń dla IOD z sektora publicznego. W ramach tego projektu przeszkoleni zostali również wybrani pracownicy urzędów ochrony danych osobowych, którzy przeprowadzili 4 szkolenia dla administracji publicznej w swoim macierzystym

kraju. W Polsce szkolenia te odbyły się na przełomie maja i czerwca 2019 r. w Poznaniu, Gdyni, Rzeszowie i Warszawie. W ramach projektu „T4DATA" powstała w Urzędzie platforma e-learningowa w oparciu o Learning Management System „Moodle", z wykładami online poświęconymi właściwemu wdrożeniu RODO w podmiotach z sektora publicznego[233]. Jej celem jest ułatwienie organom nadzorczym ds. ochrony danych tych państw oraz inspektorom ochrony danych z podmiotów publicznych, w sposób zautomatyzowany, dostępu do wiedzy o praktycznych konsekwencjach stosowania RODO i możliwych interpretacjach jego przepisów. Platforma została dostosowana do założeń projektu poprzez konfigurację mechanizmów związanych z projekcją filmów z wykładami, testów sprawdzających poziom opanowania obejrzanego wykładu wraz z informacją zwrotną po ich wypełnieniu oraz samodzielną ocenę obejrzanego wykładu przez uczestnika szkolenia. Użytkownicy platformy po wysłuchaniu każdego wykładu mogli zweryfikować swoją wiedzę przystępując do testu sprawdzającego. Projekt „T4DATA" współfinansowany jest przez Komisję Europejską w ramach Programu „Prawa, równość i obywatelstwo na lata 2016-2020".

3) **Ogólnopolski program edukacyjny TDTS**

IX edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli" w roku szkolnym 2018/2019 oraz rozpoczęcie X edycji w roku szkolnym 2019/2020.

Podniesienie kompetencji pedagogów i nauczycieli oraz edukowanie dzieci i młodzieży, jak mają chronić dane osobowe zarówno w realnym, jak i cyfrowym świecie, to główne cele tego programu, prowadzonego od 10 lat przez organ właściwy w sprawie ochrony danych osobowych, przy wsparciu Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

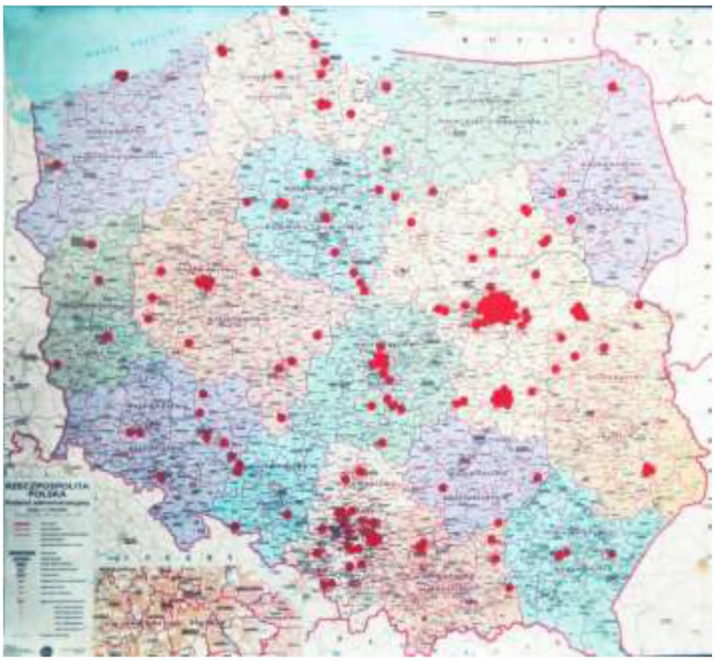
Głównym celem programu, jest poszerzenie oferty edukacyjnej placówek doskonalenia zawodowego nauczycieli oraz szkół o treści związane z ochroną danych osobowych i prawem każdego człowieka do prywatności.

Program „TDTS" – skierowany do szkół podstawowych, ponadpodstawowych oraz ośrodków doskonalenia nauczycieli – jest systemowym projektem edukacyjnym Urzędu Ochrony Danych Osobowych realizowanym na skalę ogólnopolską. Rocznie przystępuje do niego ponad 300 placówek, które podejmują różne działania edukacyjne na rzecz upowszechniania wiedzy

[233] https://t4data.uodo.gov.pl/.

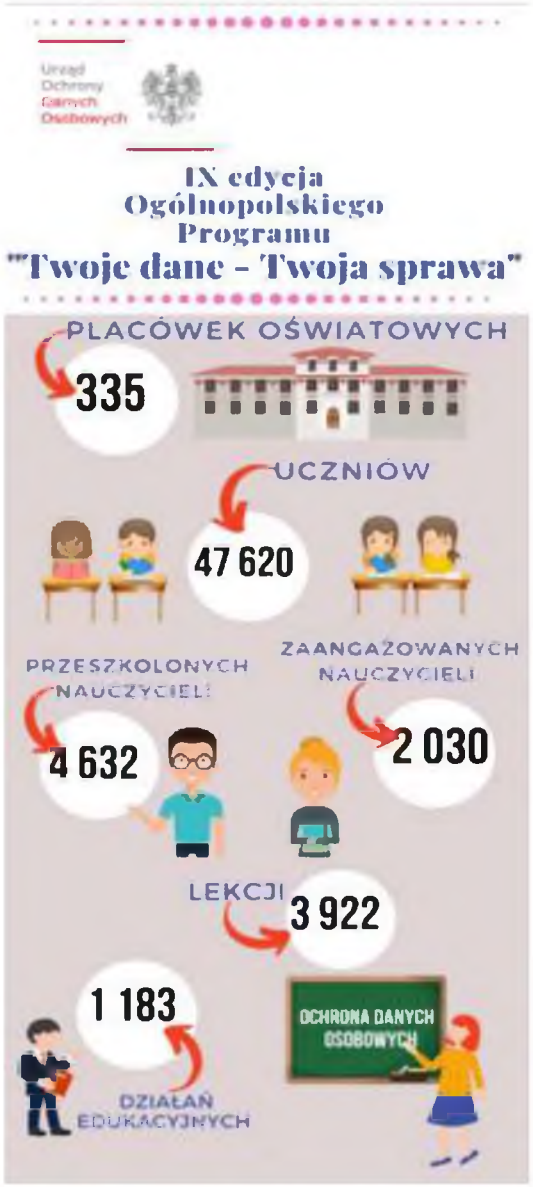
o ochronie danych osobowych i prawa do prywatności zarówno w szkołach w całej Polsce, jak i w lokalnych społecznościach. Statystycznie co roku program jest realizowany przez 3000 nauczycieli oraz 40 000 uczniów. Jednym z etapów programu jest przeszkolenie i wyposażenie kadry pedagogicznej szkół i placówek 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. „TDTS" stanowi inspirację dla nauczycieli, uczniów i rodziców, którzy pokazują, w jaki sposób od najmłodszych lat można uczyć dzieci zasad ochrony danych osobowych, przekazując trudne treści podczas zajęć lekcyjnych, pozalekcyjnych oraz innych wydarzeń tematycznych przy wykorzystaniu gier i zabaw.

W IX edycji programu „Twoje dane – Twoja sprawa", realizowanego w roku szkolnym 2018/2019, program realizowało ok. 2000 nauczycieli i ponad 45 000 uczniów z 335 placówek oświatowych z całego kraju. Wśród nich znalazło się 330 szkół i 5 ośrodków doskonalenia nauczycieli.



Mapa Polski obrazująca zasięg IX edycji programu „TDTS".

Do IX edycji programu przystąpiły placówki ze wszystkich województw, w tym 52 % placówek przystąpiło po raz pierwszy. Co roku do programu najwięcej przystępuje szkół podstawowych; w tej edycji projektu 59 % placówek też stanowiły szkoły podstawowe.



Podczas trwania IX edycji „TDTS" odbyło się około **4000 lekcji** poświęconych ochronie danych osobowych i prywatności, podczas godzin wychowawczych, informatyki i innych lekcji przedmiotowych, **4632 nauczycieli skorzystało ze szkoleń** oferowanych w ramach programu, zaś **ok. 2000 nauczycieli** aktywnie zaangażowało się w realizację różnorodnych inicjatyw edukacyjnych, w które włączyła się społeczność szkolna i środowisko lokalne. Odbywały się m.in. liczne konkursy, pikniki szkolne, konferencje, szkolenia, warsztaty, spotkania z ekspertami, happeningi, bale, pogadanki, apele, gry szkolne i przedstawienia skierowane nie tylko do uczniów i rodziców, ale także do społeczności lokalnej.

Podjęto **1183 działania edukacyjne**, w tym **410 z okazji Dnia Ochrony Danych Osobowych.** Placówkom uczestniczącym w projekcie Urząd Ochrony Danych Osobowych zapewnił materiały edukacyjne i specjalistyczne szkolenia, organizując np. cykl wykładów otwartych poświęconych m.in. praktycznym aspektom stosowania rozporządzenia ogólnego o ochronie danych osobowych.

Na szczególną uwagę zasługują dwie bardzo ciekawe inicjatywy edukacyjne, które miały miejsce podczas IX edycji programu „TDTS".

Jedną z nich była II edycja **programu sprawnościowego** autorstwa nauczyciela ze Szkoły Podstawowej nr 202 im. Jana Pawła II w Zespole Szkolno – Przedszkolnym nr 2 w Łodzi. Celem programu sprawnościowego – do którego zgłosiło się 74 szkoły – było budowanie „małych struktur UODO" w szkole i realizacja zadań w ramach programu „Twoje dane – Twoja sprawa" przez

uczniów zbierających sprawności. Sprawności, jakie można było zdobyć, to: 1) STRAŻNIK PRAWA – uczniowie, którzy respektują przepisy prawa dotyczące ochrony danych osobowych i uświadamiają innych o konieczności ich stosowania. 2) WYDAWCA – PUBLIKATOR – uczniowie, którzy przygotowują różne materiały tekstowo-graficzno-multimedialne na temat ochrony danych osobowych, opiekują się tablicami informacyjnymi, szkolną stroną internetową. 3) FOTOREPORTER – ZDOBYWCA – uczniowie, którzy wykonują dokumentację fotograficzną, prowadzą wywiady, ankiety czy inne podobne działania. 4) KRONIKARZ – WYDAWCA – uczniowie, którzy biorą udział w powstaniu kroniki – albumu działań grupy. 5) RZECZNIK – ZNAWCA – uczniowie, którzy są medialni i potrafią zaprezentować działania grupy według potrzeb. 6) ORGANIZATOR – ZWIADOWCA – uczniowie, którzy uczestniczą w sferze organizacyjnej imprez szkolnych i pozaszkolnych związanych z ochroną danych osobowych i prawa do prywatności. 7) SPECJALISTA – ZNAWCA – uczniowie kreatywni, którzy potrafią zaproponować rozwiązanie problemu.

W praktyce program ten okazał się dużym wyzwaniem. Spośród 75 szkół, które do niego przystąpiły, tylko 29 z nich w pełni zaangażowało się i zrealizowało jego założenia, przechodząc przez wszystkie etapy i zdobywając tytułu „Znawcy RODO". Każdy etap tej inicjatywy wymagał od szkolnego koordynatora i uczniów dużej dyscypliny organizacyjnej przy realizacji poszczególnych zadań oraz ogromnego zaangażowania grup szkolnych na przestrzeni całego roku szkolnego. Podczas spotkania podsumowującego IX edycję programu „TDTS" szkoły, które ukończyły II edycję programu sprawnościowego, zostały wyróżnione statuetką, otrzymując tytuł „ZNAWCY RODO", natomiast najbardziej aktywni liderzy grup szkolnych – uczniowie otrzymali medale i tytuł „MŁODEGO INSPEKTORA OCHRONY DANYCH".

Drugą ze wspomnianych inicjatyw była **XV PREZENTACJA AKTYWNOŚCI KULTURALNEJ SZKÓŁ URSUSA PAKSU 2019** zorganizowana 29 maja 2019 r. pod honorowym patronatem Rady i Zarządu Dzielnicy Ursus m.st. Warszawa w Ośrodku Kultury „Arsus". Wśród prezentacji umiejętności wokalnych, instrumentalnych, recytatorskich, tanecznych i akrobatycznych, został zaprezentowany projekt „Udany Oficjalny Debiut Oryginalny – Nasze wybory". Ten innowacyjny projekt powstał w Szkole Podstawowej Nr 360 w Warszawie w ramach programu „Twoje dane – Twoja sprawa". Dzięki zaangażowaniu uczniów i nauczycieli z dzielnicy Ursus, został opublikowany wyjątkowy zbiór prac literackich. W książce tej zamieszczono osobiste refleksje dzieci i młodzieży na temat ochrony danych wrażliwych, podsumowując tym samym pierwszy rok funkcjonowania RODO oraz list Prezesa Urzędu Ochrony

Danych Osobowych, w którym dziękuje dyrektorom, uczniom i koordynatorom programu „TDTS" ursuskich szkół za zaangażowanie i wysiłek wkładany na rzecz upowszechnienia wiedzy wśród uczniów i nauczycieli, w celu poprawy jakości ochrony danych osobowych oraz kształtowania właściwych postaw.

Podczas IX edycji „TDTS" odbyły się także dwa spotkania z **cyklu konferencji wojewódzkich**, prezentujące placówkom oświatowym z niewielkich miejscowości cele i zasady udziału w tym programie. Pierwsze z tych spotkań odbyło się w Siedlcach (29.03.2019 r.), drugie – w Sieradzu (3.04.2019). Podkreślenia wymaga, że wydarzenie w Sieradzu było pierwszym i jedynym w województwie łódzkim spotkaniem z ochroną danych osobowych w szkole. Spotkania, w których uczestniczyło ok. 500 przedstawicieli szkół, stanowiły doskonałą okazję do rozmów, zdobycia wiedzy oraz refleksji na temat realizacji prawa do prywatności uczniów oraz ochrony i bezpieczeństwa danych osobowych w szkołach.

Program „Twoje dane – Twoja sprawa" cieszy się niesłabnącym zainteresowaniem placówek oświatowych, czego dowodem jest rozpoczęcie kolejnej, **dziesiątej jego edycji na rok szkolny 2019/2020.** Żeby utrwalić ten efekt i wzmocnić jeszcze bardziej rozpoznawalność programu, wraz z jubileuszową edycją programu zaczął być stosowany nowy system identyfikacji wizualnej w postaci **nowego logotypu „TDTS".** Dodatkowo, w celu zapewnienia lepszej rozpoznawalności programu w Internecie, informacje o zrealizowanych wydarzeniach będą dostępne także pod hasztagiem – **#TwojedaneTwojasprawa**.

Do X edycji programu „TDTS" zgłosiły się 343 szkoły, w tym 10 ośrodków szkolenia nauczycieli.

Konferencja z cyklu #RODO w edukacji, która odbyła się **1 października 2019 r. w Rojowie** (woj. wielkopolskie), zainaugurowała realizację jubileuszowej, X edycji programu „TDTS", dzięki współpracy Jana Nowaka, Prezesa Urzędu Ochrony Danych Osobowych oraz senatora Łukasza Mikołajczyka, Przewodniczącego Senackiego Zespołu ds. Bezpieczeństwa Dzieci i Młodzieży w Świecie Wirtualnym. Wydarzenie to było okazją do przedyskutowania w gronie ekspertów kluczowych zagadnień z zakresu ochrony danych osobowych w szkołach i placówkach oświatowych. Eksperci omówili wybrane zagadnienia z zakresu przetwarzania danych osobowych uczniów przez szkołę oraz zapoznali się z zadaniami organu nadzorczego w zakresie edukacji.

Ważnym elementem realizacji każdej edycji programu są inicjatywy edukacyjne przygotowane przez szkoły, które w ten sposób promują ideę ochrony prywatności wśród uczniów i nauczycieli. W trakcie spotkania w Rojowie zaprezentowały się trzy szkoły z Wielkopolski:

Szkoła Podstawowa ze Świby, Szkoła Podstawowa z Oddziałami Integracyjnymi im. Powstańców Wielkopolskich z Nowych Skalmierzyc oraz XXXI Liceum Ogólnokształcące w Zespole Szkół Handlowych im. Bohaterów Poznańskiego Czerwca '56 z Poznania.

Z kolei **2 i 3 października 2019 r. w Senacie** RP odbyło się kolejne, kluczowe wydarzenie związane z programem – szkolenie dla koordynatorów ze szkół i placówek oświatowych, które zgłosiły uczestnictwo w programie w roku szkolnym 2019/2020. Szkolenie służy przygotowaniu nauczycieli do kształtowania świadomych i odpowiedzialnych postaw wśród uczniów w zakresie ochrony prywatności i danych osobowych. Koordynatorom programu przekazano niezbędną wiedzę dotyczącą ochrony danych osobowych, dodatkowo wyposażając kadrę pedagogiczną szkół i placówek doskonalenia nauczycieli w materiały edukacyjne. Uczestnicy wydarzenia poznali też wybrane inicjatywy edukacyjne, realizowane w poprzednich edycjach programu. Do ich dyspozycji byli także eksperci UODO, z którymi mogli skonsultować wiele zagadnień z zakresu ochrony danych osobowych w oświacie.

Program „Twoje dane – Twoja sprawa" to projekt edukacyjny, który jednocześnie stwarza warunki do tworzenia sieci współpracy, wymiany poglądów i dobrych praktyk w zakresie edukacji uczniów oraz wymiany doświadczeń. Przyczynia się do kształtowania odpowiednich nawyków i właściwego stosowania zdobytej wiedzy w życiu codziennym przez uczniów. Program to także okazja do dobrej i owocnej współpracy z wieloma urzędami i instytucjami na rzecz ochrony prywatności i praw dzieci oraz krzewienia wartości ochrony danych osobowych oraz edukacji prawnej wśród uczniów, nauczycieli, rodziców i środowiska lokalnego na terenie całego kraju, a tym samym promocji szkoły bezpiecznej, aktywnej i zaangażowanej. Zadanie to ułatwia specjalna platforma programu „TDTS", uruchomiana na stronie internetowej UODO. W 2019 r. system „TDTS" został znacznie rozbudowany o wiele nowych funkcjonalności, które umożliwiły szkołom rejestrację przez cały rok, w miejscu poprzedniej rejestracji do określonego dnia. Zmiana ta miała znaczny wpływ na procesy przesyłania informacji do uczestników programu. Ponadto szkoły uczestniczące w programie otrzymały swój profil, a pojedynczy koordynator otrzymał możliwość zarządzania kilkoma placówkami. Rozszerzono także możliwości zarządzania zgłoszonymi inicjatywami. Koordynatorzy mogą teraz sami korygować teksty zgłoszonych inicjatyw. Dodano moduł tablicy informacyjnej, który rozwiązał problemy związane z informowaniem szkół o różnych wydarzeniach, w zależności od momentu przystąpienia do programu „TDTS".

1.4. Porozumienia o współpracy

1) Kościelny Inspektor Ochrony Danych, 10.05.2019 r.

Prezes Urzędu Ochrony Danych oraz Kościelny Inspektor Ochrony Danych zawarli 10 maja 2019 r. w Warszawie porozumienie o współpracy i wzajemnym przekazywaniu informacji.

Porozumienie określa zasady, zakres i formę współpracy pomiędzy Prezesem UODO i Kościelnym Inspektorem Ochrony Danych – niezależnym organem nadzorczym w zakresie ochrony danych osobowych Kościoła katolickiego. Porozumienie dotyczy realizacji przewidzianych prawem zadań obu organów, z poszanowaniem ich niezależności i kompetencji. Kościoły i związki wyznaniowe są zobowiązane do przestrzegania ogólnego rozporządzenia o ochronie danych (RODO). Jednak te, które w momencie wejścia w życie RODO (a więc 25 maja 2018 r.) stosowały już wewnętrzne zasady ochrony danych osobowych, mogą – zgodnie z art. 91 ust. 1 RODO – nadal stosować własne regulacje w tym zakresie. Muszą być one jedynie dostosowane do RODO. Przepisy Porozumienia przewidują podejmowanie wspólnych działań, zmierzających do zapewnienia spójnego stosowania prawa w zakresie ochrony danych osobowych przez podmioty kościelne i zobowiązują do współpracy, w szczególności w zakresie działań edukacyjnych i informacyjnych dotyczących praw osób fizycznych w zakresie prawa do prywatności i ochrony danych osobowych. Dokument podpisali: dr Edyta Bielak-Jomaa, Prezes Urzędu Ochrony Danych Osobowych oraz ks. dr hab. Piotr Kroczek, Kościelny Inspektor Ochrony Danych.

2) Krajowa Szkoła Administracji Publicznej im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego (KSAP), 7.11.2019 r.

Porozumienie o współpracy w zakresie ochrony prywatności i danych osobowych pomiędzy Urzędem Ochrony Danych Osobowych a Krajową Szkołą Administracji Publicznej (KSAP) zostało podpisane 7 listopada 2019 r. w Warszawie. Podejmowanie wspólnych działań na rzecz podnoszenia poziomu wiedzy o ochronie prywatności i danych osobowych oraz wymiana doświadczeń – to główne cele zawartego porozumienia. Współpraca obejmować będzie działalność naukowo-badawczą, edukacyjną i szkoleniową, promocyjną, wydawniczą i organizacyjną. Porozumienie przewiduje m.in. realizację wspólnych projektów, wymianę materiałów o charakterze analitycznym i informacyjnym, inicjowanie prac naukowych i badawczych z zakresu ochrony danych osobowych oraz współorganizowanie seminariów, konferencji naukowych i szkoleń. Walor edukacyjny porozumienia podkreślała w szczególności deklaracja współpracy przy organizacji studium szkoleniowych z zakresu ochrony danych osobowych dla słuchaczy KSAP. Przy wsparciu

merytorycznym Urzędu, w roku akademickim 2019/2020 uruchomiona została 3. edycja Studium dla Inspektorów Ochrony Danych w sektorze publicznym. Uroczystość inauguracji 3. edycji tego Studium odbyła się 9.12.2019 r. z udziałem przedstawicieli UODO.

1.5. Publikacje

„Podręcznik Inspektora Ochrony Danych" to zbiór wytycznych dla IOD dotyczących sposobu zapewnienia zgodności z ogólnym rozporządzeniem o ochronie danych (RODO). Poradnik ten opracowany został w ramach projektu „T4DATA" i jest dostępny w polskiej i angielskiej wersji językowej[234]. Podręcznik pomoże zwiększyć świadomość i rozumienie roli, kompetencji i głównych obowiązków inspektorów ochrony danych oraz ułatwić tworzenie europejskiej kultury monitorowania, przeglądu i oceny przetwarzania danych. Może też być pomocny w określeniu, jak w kontekście RODO należy patrzeć na status i gwarancje związane z pełnieniem funkcji inspektora ochrony danych. Publikacja ma charakter pomocniczy i zawiera wskazówki, których zastosowanie w konkretnym przypadku może wymagać dodatkowej analizy. Dlatego opublikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organu nadzorczego. Poradnik jest elementem materiałów szkoleniowych dla trenerów w ramach międzynarodowego projektu „T4DATA", a wraz z platformą edukacyjną z wykładami dla inspektorów ochrony danych stanowi rezultaty tego przedsięwzięcia.

1.6. Filmy edukacyjne

Organ ds. ochrony danych osobowych wskazuje, że w wielu przypadkach, w których pojawiają się wątpliwości związane ze stosowaniem ogólnego rozporządzenia, pomocne w analizie danej sytuacji czy też – doborze odpowiednich środków ochrony danych – są zarówno wytyczne Europejskiej Rady Ochrony Danych, jak i przygotowane przez Urząd Ochrony Danych Osobowych publikacje i filmy o charakterze edukacyjnym. W analizowanym 2019 roku Urząd przygotował i opublikował na swojej stronie internetowej cykl filmów edukacyjnych pomocnych we właściwym rozumieniu i stosowaniu przepisów ogólnego rozporządzenia, w wybranych obszarach działalności różnych podmiotów.

Dotychczas ukazały się następujące filmy edukacyjne:

- Dowód zawsze osobisty. Sprawdź, jak go chronić[235],
- W oku kamery. Monitoring wizyjny – Prezes UODO wyjaśnia, jak go obecnie stosować[236],

[234] https://uodo.gov.pl/pl/168/1298
[235] https://uodo.gov.pl/pl/384/710

- Przychodzi pacjent do lekarza… i na co musi zwrócić uwagę, by chronić swoje dane?[237],
- Szkoła uczy (się) chronić dane[238].

1.7. Konferencje, seminaria, spotkania

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

Poniżej przedstawione zostały wybrane przykłady wydarzeń o charakterze ogólnopolskim lub międzynarodowym z udziałem Prezesa UODO bądź jego przedstawicieli, które odbyły się w Polsce. Ich pełny wykaz zawiera załącznik nr 3.

1) XIII Dzień Ochrony Danych Osobowych – 28 stycznia 2019 r.

Przypadające co roku **28 stycznia** święto Dzień Ochrony Danych Osobowych, zostało ustanowione dla upamiętnienia rocznicy otwarcia do podpisu Konwencji 108 Rady Europy w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych – najstarszego aktu prawnego o zasięgu międzynarodowym, kompleksowo regulującego zagadnienia związane z ochroną 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. Z tej okazji w całej Europie organizowane są różne wydarzenia poświęcone aktualnym zagadnieniom związanym z prawem do prywatności i ochrony danych osobowych, informujące obywateli w zakresie ich praw i obowiązków oraz zagrożeń związanych z przetwarzaniem dotyczących ich danych osobowych.

Główne obchody Dnia Ochrony Danych Osobowych – organizowane przez UODO – odbyły się 28 stycznia 2019 r. w Warszawie. Ich głównym punktem była konferencja pt. „System ochrony danych osobowych po wprowadzeniu reformy", poświęcona praktycznym aspektom wdrożenia RODO. Podczas spotkania eksperci Urzędu oraz zaproszeni praktycy dyskutowali o aktualnych zagadnieniach związanych z prawem do prywatności i ochrony danych osobowych w kontekście doświadczeń związanych ze stosowaniem od 25 maja 2018 r. ogólnego rozporządzenia o ochronie danych. Główne zagadnienia konferencji dotyczyły wdrożenia dyrektywy 2016/680 (dyrektywy

[236] https://uodo.gov.pl/pl/384/723
[237] https://uodo.gov.pl/pl/384/738
[238] https://uodo.gov.pl/pl/384/742

policyjnej) w Polsce, telemarketingu oraz zagadnień związanych z realizacją praw osób w Internecie. Prezes UODO w swoim wystąpieniu otwierającym to wydarzenie podkreśliła, że po siedmiu miesiącach obowiązywania nowego prawa o ochronie danych osobowych w polskim porządku prawnym, już czas najwyższy zacząć rozmawiać o **systemie ochrony danych**, a nie jedynie o rozporządzeniu. Zaapelowała przy tym do przedstawicieli władz publicznych, by wspierali Urząd i jego działania dla dobra wszystkich obywateli oraz dla zagwarantowania przestrzegania ochrony danych osobowych jako standardu na wszystkich możliwych poziomach. Na zakończenie wskazała trzy tematy, które będą bardzo ważne w najbliższym czasie z punktu widzenia danych osobowych, a mianowicie: przestrzeganie praw gwarantowanych przez RODO w branży telemarketingowej, przygotowania do brexitu i nadchodzące podwójne wybory.

Dzień Ochrony Danych Osobowych był również okazją do wręczenia przez Prezes UODO Nagrody im. Michała Serzyckiego, Generalnego Inspektora Ochrony Danych Osobowych III Kadencji[239].

Tradycyjnie też, z okazji tego święta, UODO podejmował inne działania mające na celu zwrócenie uwagi na potrzebę ochrony prywatności i danych osobowych, np. akcje informacyjno-edukacyjne w placówkach oświatowych uczestniczących w IX edycji programu edukacyjnego UODO „Twoje dane – Twoja sprawa". Wśród wielu inicjatyw, które szkoły realizowały w ramach obchodów tego święta było m.in. słuchowisko, gry miejskie, konkursy wiedzy oraz wizyty w instytucjach publicznych.

Wzorem lat ubiegłych, w obchody tego święta zaangażowały się też uczelnie wyższe, z którymi UODO ma zawarte porozumienia o współpracy. Dla przykładu Akademia Wyższej Szkoły Biznesu w Dąbrowie Górniczej zorganizowała pod patronatem Prezes UODO **V Dzień Otwarty Urzędu Ochrony Danych Osobowych** (1.02.2019) – konferencję tematyczną połączoną z promocją dobrych praktyk w zakresie ochrony danych osobowych. Na uwagę zasługuje także inicjatywa **Śląskiej Sieci Metropolitalnej z Gliwic**, która przygotowała ogólnopolską kampanię na temat bezpieczeństwa w sieci. Wraz z gliwicką Biblioteką Publiczną zorganizowała konkurs dla uczniów i studentów, pod honorowym patronatem Prezesa UODO, na opracowanie spotu reklamowego promującego ideę ochrony danych osobowych. W ramach kampanii najlepsze spoty trafiły do szkół, gdzie na ogólnodostępnych telebimach były emitowane 28 stycznia 2019 r. mieszkańcom Warszawy, Poznania, Krakowa, Katowic, Wrocławia, Opola, Bydgoszczy i Gdańska.

[239] Więcej na ten temat w komunikacie pod linkiem: https://uodo.gov.pl/pl/226/688.

2) **Konferencja „Wdrożenie RODO w sektorze medycznym – gdzie jesteśmy, dokąd zmierzamy? – edycja II". Warszawa, 27.02.2019 r.**

Przedstawiciel UODO został zaproszony do udziału w sesji poświęconej opracowaniu kodeksu postępowania w sektorze ochrony zdrowia. Konferencja była miejscem oficjalnego otwarcia ogólnopolskiej kampanii edukacyjnej pt. „rododlapacjenta.pl", która objęta została patronatem Prezesa UODO. Podczas tego wydarzenia przekazane zostały informacje o nowych regulacjach obowiązujących podmioty wykonujące działalność leczniczą, dotyczących cyberbezpieczeństwa. Podjęte również zostały tematy związane z bezpiecznym korzystaniem z nowych technologii i innowacjami w zdrowiu, jak telemedycyna, e-recepty czy sztuczna inteligencja. Organizatorami Konferencji byli: Uczelnia Łazarskiego, Polska Federacja Szpitali oraz Domański Zakrzewski Palinka Sp.k.

3) **Spotkanie edukacyjne „360° Master Panel". Warszawa, 1.03.2019 r.**

Towarzystwo Chirurgów Polskich oraz Johnson & Johnson Sp. z o.o. byli organizatorami spotkania edukacyjnego lekarzy chirurgów w celu omówienia najnowszych standardów w chirurgii ogólnej. Jedna z sesji tego spotkania poświęcona była roli certyfikacji w chirurgii bariatrycznej oraz prowadzeniu rejestrów, jako narzędzia kontroli jakości usług medycznych. Przedstawiciel Zespołu ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa UODO przedstawił aspekt ochrony danych osobowych w odniesieniu do rejestrów medycznych. Jest to zagadnienie bardzo ważne w obliczu planów Ministra Zdrowia, utworzenia wielu rejestrów medycznych, w tym rejestru bariatrycznego, którego prowadzeniem zajmowałoby się Towarzystwo Chirurgów Polskich.

4) **Seminarium Naukowe dla studentów trzech wydziałów prawa. Warszawa, 25.03.2019 r.**

Studenci trzech kół naukowych: Studenckiego Koła Naukowego Prawa Nowych Technologii Uniwersytetu Mikołaja Kopernika w Toruniu, Koła Naukowego Prawa Własności Intelektualnej, Mediów i Internetu Uniwersytetu w Białymstoku oraz Koła Naukowego Prawa Własności Intelektualnej i Prawa Nowych Technologii Uniwersytetu Gdańskiego, przyjechali do Warszawy na zorganizowane przez UODO Seminarium Naukowe. Podczas tego spotkania przedstawiciele kół wygłosili prezentacje dotyczące „Przetwarzania danych osobowych kandydatów do pracy w procesie rekrutacji", „Instytucji powierzenia przetwarzania danych osobowych" oraz „Przetwarzania danych w grupach kapitałowych", które były moderowane przez dyrektorów zespołów UODO. Było to drugie już tego rodzaju seminarium zorganizowane przez Urząd specjalnie dla studentów. Poprzednie odbyło się 23 maja 2014 r. na zaproszenie dr Wojciecha

R. Wiewiórowskiego, Generalnego Inspektora Ochrony Danych Osobowych IV kadencji, obecnie Europejskiego Inspektora Ochrony Danych Osobowych (2019-2024).

5) Konferencja „Podsumowanie pierwszego roku obowiązywania RODO w jednostkach samorządu terytorialnego – JST". Warszawa, 10.03.2019 r.

Urząd Ochrony Danych Osobowych, Sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej oraz Narodowy Instytut Samorządu Terytorialnego – NIST, wspólnie podsumowali pierwszy rok obowiązywania RODO w jednostkach samorządu terytorialnego – JST. Rejestry mieszkańców, monitoring wizyjny, zasoby BIP oraz stron internetowych urzędów – w tych obszarach samorządowcy mieli największe problemy ze stosowaniem ogólnego rozporządzenia o ochronie danych osobowych. Natomiast administratorzy w JST powinni inwestować w edukację personelu (w tym kierownictwa) z zakresu ochrony danych osobowych, a także rozważyć tworzenie kodeksów postępowań. Takie wnioski wyniknęły z konferencji podsumowującej pierwszy rok obowiązywania RODO w jednostkach samorządu terytorialnego. Podczas tego wydarzenia wręczone zostały nagrody dla laureatów IX edycji konkursu na esej dla studentów wydziałów prawa i administracji[240], którego organizatorem był Urząd Ochrony Danych Osobowych.

6) „#RODO w edukacji". Sieradz, 3.04.2019 r.

Prywatność dzieci była wiodącym tematem spotkania „#RODO w edukacji", które odbyło się 3 kwietnia 2019 r. w Sieradzu. To kolejna z cyklu konferencji wojewódzkich Urzędu Ochrony Danych Osobowych, których celem było zapoznanie dyrektorów oraz nauczycieli szkół i placówek oświatowych z ogólnopolskim programem edukacyjnym UODO „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Celem tego programu jest podnoszenie wiedzy dotyczącej ochrony danych osobowych i prawa do prywatności – zarówno wśród nauczycieli, jak i uczniów oraz w całym środowisku lokalnym. Uczestnicy spotkania w Sieradzu mieli możliwość poznania praktycznych aspektów ochrony danych osobowych w działalności szkół, jak obowiązek informacyjny czy monitoring w szkole. Sieradzkie spotkanie UODO organizował wspólnie z Urzędem Marszałkowskim Województwa Łódzkiego. Łódzka szkoła jest jedną z 334 placówek edukacyjnych z całej Polski, które uczestniczą w programie „Twoje dane – Twoja sprawa".

[240] https://uodo.gov.pl/pl/138/1055

7) VI Forum Kierowników IT w Administracji. Zakopane, 11.04.2019 r.

Forum Kierowników IT w Administracji to już szósta edycja ogólnopolskiej konferencji dla osób odpowiedzialnych za informatyzację instytucji publicznych. Tematem przewodnim tego wydarzenia były bezpieczne, wydajne i efektywne usługi elektroniczne w administracji publicznej. Ponadto poruszone zostały zagadnienia, takie jak: strategiczne kierunki transformacji cyfrowej administracji publicznej wynikające z nowego programu Zintegrowanej Informatyzacji Państwa, wyzwania dla urzędów w związku z wdrażaniem przepisów ustawy o Krajowym Systemie Cyberbezpieczeństwa, wpływ RODO na dostęp do informacji publicznej oraz na jej ponowne wykorzystanie. Przedstawiciel UODO przedstawił prezentację dotyczącą naruszeń ochrony danych osobowych z perspektywy organu nadzorczego z uwzględnieniem roli działów IT sektora publicznego.

8) Konferencja „Ochrona danych medycznych w dobie nowych technologii". Kraków, 12.04.2019 r.

Prywatność danych i bezpieczeństwo w opiece zdrowotnej, procedury weryfikacji zgodności z RODO – były tematem wystąpienia przedstawiciela Urzędu podczas tej konferencji. Poruszone zostały też zagadnienia związane ze zwalnianiem z tajemnicy zawodowej lekarza przez osoby bliskie po śmierci pacjenta, w oparciu o nowe przepisy oraz ochrona danych medycznych w kontekście wykorzystania technologii blockchain w medycynie w ramach „smart contract". W agendzie zaplanowane były również wykłady dotyczące ochrony danych osobowych w przypadku zastosowania rozwiązań telemedycznych, sztucznej inteligencji (AI) oraz Internet of Body. Organizatorem Konferencji było Koło Naukowe Prawa Medycznego Uniwersytetu Jagiellońskiego.

9) XI Międzynarodowa Konferencja Naukowa „Ochrona praw człowieka w dobie kryzysu demokracji liberalnej". Warszawa, 15.04.2019 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 pt. „Ochrona praw człowieka w dobie kryzysu demokracji liberalnej". Jedenasta edycja tej Międzynarodowej Konferencji poświęcona była obchodom 70. rocznicy powstania Rady Europy, 10-lecia wejścia w życie Traktatu z Lizbony i 15-lecia członkostwa Polski w Unii Europejskiej. Wystąpienie otwierające wygłosiła dr Edyta Bielak-Jomaa, Prezes UODO, podkreślając znaczenie aktów prawa europejskiego

i międzynarodowego dla ochrony prawa człowieka. Prelegentami tej Konferencji byli naukowcy z Polski, Hiszpanii, Kazachstanu, Litwy, Rosji, Serbii, Słowacji, Stanów Zjednoczonych i Ukrainy.

10) „Impact'19". Kraków, 22.05.2019 r.

Konferencja gospodarcza „Impact'19" odbywała się w świetle polsko-francuskiego roku nauki i obchodów 100-lecia AGH. Jedna z ośmiu ścieżek tematycznych „Impact'19" dotyczyła wykorzystania potencjału sztucznej inteligencji (AI) w sektorze medycznym i farmaceutycznym w Polsce. Przedstawiciel UODO wystąpił w panelu dyskusyjnym pt. „Dlaczego potrzebujemy strategii AI w zdrowiu?", gdzie sygnalizował, że jednym z kluczowych wyzwań i barier związanych z rozwojem algorytmów sztucznej inteligencji w Polsce jest kwestia dostępu do jakościowych danych medycznych z zapewnieniem praw i wolności osób, których dane dotyczą. Konieczne jest także ustalenie ram regulacyjnych dotyczących wykorzystania AI w sektorze medycznym i farmaceutycznym, z uwzględnieniem bezpośredniego wpływu technologii AI na ochronę życia i zdrowia ludzi. Organizatorzy: Fundacja Impact, Kancelaria Domański Zakrzewski Palinka Sp.k.

11) Spotkanie pt. „RODO już rok z nami. Projekt e-OpenSpace". Warszawa, 30.05.2019 r.

Podsumowanie doświadczeń z 12 miesięcy stosowania RODO oraz prezentacja powstającej europejskiej platformy e-learningowej poświęconej ochronie danych osobowych, były głównymi tematami spotkania „RODO już rok z nami. Projekt e-OpenSpace". Organizatorem tego wydarzenia był Urząd Ochrony Danych Osobowych przy współpracy Uniwersytetu Jagiellońskiego. Podczas spotkania podkreślano ważną rolę wytycznych Europejskiej Rady Ochrony Danych – EROD, bez których krajowe organy ochrony danych narażone były na działania uniemożliwiające osiągnięcie spójności. Wskazywano, że również UODO podjął i nadal realizuje wiele działań, które ułatwiają stosowanie RODO. Wśród nich są m.in. poradniki i wytyczne, szkolenia branżowe, a także działanie infolinii. Dzięki takim działaniom możliwe jest ograniczenie zjawiska „dzikiej wiedzy", z którym mamy do czynienia wtedy, gdy ludzie przyjmując wiedzę o akcie prawnym, wytwarzają na jego temat fałszywe przekonania. Jest to powszechne i nieuniknione zjawisko, dlatego edukacja prawnicza jest niezbędna, aby rozwiać pojawiające się wątpliwości.

12) VI Kongres Zarządzania Administracją Samorządową. Wrocław, 5.06.2019 r.

Zarządzanie funkcjonowaniem administracji samorządowej nie jest zadaniem łatwym, jeśli weźmie się pod uwagę zakres działań i zadań, jakie stoją przed nowocześnie zarządzanym samorządem. Dlatego podczas Kongresu poruszone były różnorodne tematy – od przepisów prawa pracy i zarządzania ścieżką kariery pracowników, poprzez zarządzanie informacją publiczną,

wykorzystywaniem rozwiązań sztucznej inteligencji (AI), a na obsłudze informatycznej urzędu i szukaniu systemowych rozwiązań zwiększających dostępność oraz jakość danych publicznych, kończąc. Przedstawiciel UODO wystąpił w panelu poświęconym RODO i udostępnianiu informacji publicznej, gdzie przedstawił kwestie związane z odmową udostępnienia, w szczególności w kontekście prawa do prywatności i ochrony danych osobowych. Przedstawił również praktyczne problemy związane ze sprawowaniem funkcji IOD w samorządzie. Organizatorami wydarzenia była redakcja pisma samorządu terytorialnego „Wspólnota" oraz firma Municipium.

13) XI Konferencja Naukowa „Bezpieczeństwo w Internecie". Warszawa, 6-7.06.2019 r.

Tematem XI Konferencji z cyklu „Bezpieczeństwo w Internecie" była analityka danych, przedstawiona w różnorodnych aspektach. Przedstawione zostały tematy związane z przetwarzaniem danych osobowych w wielkich zbiorach danych – począwszy od istoty i znaczenia analityki danych w różnych sektorach (służba zdrowia, bankowość, ubezpieczenia, wymiar sprawiedliwości, itd.), poprzez zagadnienia dotyczące pozyskiwania danych do analizy, omówienie zagrożeń dla praw i wolności osób fizycznych, w szczególności tych związanych z przetwarzaniem danych wrażliwych czy profilowaniem, a na środkach zapewniających ich bezpieczeństwo kończąc. Podczas konferencji poruszony został temat analityki danych w kontekście zapewnienia ochrony danych osobowych – w aspekcie analizy ryzyka związanego z przetwarzaniem danych osobowych, a także zasady rozliczalności i celowości przetwarzania danych osobowych. Organizatorami Konferencji były UODO oraz UKSW. Organ właściwy do spraw ochrony danych osobowych był współorganizatorem wszystkich dorocznych edycji konferencji z cyklu „Bezpieczeństwo w Internecie', które przy wsparciu merytorycznym i organizacyjnym Urzędu odbywały się na tej uczelni.

14) Konferencja „Podsumowanie pierwszego roku obowiązywania RODO w jednostkach samorządu terytorialnego". Warszawa, 10.06.2019 r.

Obszary, w których samorządowcy mieli największe problemy ze stosowaniem przepisów ogólnego rozporządzenia o ochronie danych osobowych obejmowały: rejestry mieszkańców, monitoring wizyjny, zasoby BIP oraz stron internetowych urzędów. Takie wnioski z kontroli przeprowadzonych przez inspektorów UODO w jednostkach samorządu terytorialnego (JST) przedstawione zostały podczas tego spotkania. Przedstawiciele Urzędu zachęcali administratorów w JST do zorganizowania edukacji personelu (w tym kadry zarządzającej) z zakresu ochrony danych osobowych oraz tworzenia kodeksów postępowań przez zrzeszające je organizacje.

W ocenie prelegentów UODO kodeks postępowania jest jednym ze sposobów na zapewnienie przez samorządowców zgodności ich działań z obowiązującymi przepisami o ochronie danych. Kodeksy mogą dotyczyć realizacji odrębnych zadań publicznych, np. oświaty, pomocy społecznej, wykorzystania środków unijnych, itp. Konferencję zorganizowali: Urząd Ochrony Danych Osobowych, Sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej oraz Narodowy Instytut Samorządu Terytorialnego – NIST.

15) Konferencja dla słuchaczy st. podyplomowych WPiA UJ. Kraków, 14.06.2019 r.

„Praktyczne problemy w stosowaniu ogólnego rozporządzenia o ochronie danych – refleksje po roku doświadczeń" to tytuł Konferencji Naukowej zorganizowanej na Uniwersytecie Jagiellońskim. W zamierzeniu organizatora konferencja ta skierowana była przede wszystkim do absolwentów Studiów Podyplomowych „Bezpieczeństwo informacji w administracji i biznesie", które objęte są patronatem honorowym Prezesa UODO. Na zaproszenie Pana Profesora Tadeusza Włudyki, Kierownika Katedry Polityki Gospodarczej WPiA UJ, uczestniczyli w niej pracownicy UODO, którzy byli wykładowcami na tych studiach. W oparciu o referaty prelegentów oraz doświadczenia zawodowe słuchaczy tych studiów, przeprowadzony został panel dyskusyjny na temat problemów związanych z wdrażaniem RODO.

16) Konferencja dotycząca stosowania RODO w instytucjach finansowych. Warszawa, 27.06.2019 r.

Zmiany ustaw dostosowujących przepisy krajowe do RODO – w tym te dotyczące sektora instytucji finansowych – w związku z podpisaniem przez Prezydenta RP w dniu 4 kwietnia 2019 r. ustawy wprowadzającej te zmiany, a także wiele wytycznych i rekomendacji dotyczących stosowania przepisów RODO, wydanych zarówno na poziomie unijnym (przez Europejską Radę Ochrony Danych), jak i krajowym (Prezes UODO i Ministerstwo Cyfryzacji) było głównym powodem zorganizowania w Warszawie Konferencji poświęconej temu tematowi. Sektor finansowy jest bowiem branżą, dla której przetwarzanie danych osobowych stanowi kluczowy element większości procesów biznesowych. Problematyka sprostania wymogom RODO w instytucjach finansowych, z punktu widzenia regulatora, została przedstawiona przez przedstawiciela Urzędu Ochrony Danych Osobowych. Organizatorem tego wydarzenia był Puls Biznesu, zaś partnerem merytorycznym Kancelaria Traple Konarski Podrecki i Wspólnicy.

17) VIII Konwent Ochrony Danych i Informacji. Łódź, 19.11.2019 r.

Już po raz ósmy przedstawiciele świata nauki, biznesu i administracji spotkali się w Łodzi, by dyskutować o właściwych interpretacjach nowych rozwiązań prawnych w zakresie ochrony danych

i bezpieczeństwa informacji. Tematem tegorocznej edycji Konwentu były „D(RODO)wskazy, czyli nowe kierunki ochrony danych w biznesie", natomiast prelekcje oraz dyskusje toczyły się głównie wokół czterech zagadnień: RODO w marketingu, RODO w HR, Cyberbezpieczeństwo oraz analiza ryzyka. W drugiej części wydarzenia organizatorzy zaproponowali innowacyjną formułę, tzw. #DataProtectionMIXER, czyli bezpośrednie spotkania przy stolikach tematycznych, z udziałem ekspertów z zakresu ochrony danych i bezpieczeństwa informacji. W ramach tego wydarzenia odbyły się pierwsze w Polsce Targi Ochrony Danych Osobowych.

18) Konferencja „Analiza i bezpieczeństwo zasobów informacyjnych – problemy prawne, naukowe i techniczne". Warszawa, 26.11.2019 r.

W siedzibie ZUS odbyła się konferencja poświęcona bezpieczeństwu zasobów informacyjnych, której organizatorem był Zakład Ubezpieczeń Społecznych we współpracy z Wojskową Akademią Techniczną i Głównym Urzędem Statystycznym. Prezes UODO został członkiem Komitetu Honorowego Konferencji, której organizacja zbiegła się z obchodami 85-lecia istnienia Zakładu Ubezpieczeń Społecznych. W sesji poświęconej bezpieczeństwu danych osobowych z perspektywy doświadczeń pierwszego roku wdrożenia RODO wystąpił przedstawiciel UODO, który przybliżył zagadnienia związane z projektowaniem ochrony danych osobowych w rejestrach publicznych. Działania na rzecz bezpieczeństwa informacyjnego muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a w szczególności z poszanowaniem prawa do wolności słowa oraz prywatności i ochrony danych osobowych. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być zawsze oparta na efektywnej i wiarygodnej analizie ryzyka.

19) 24. Kongres Inspektorów Ochrony Danych. Siła k/Olsztyna, 3-5.12.2019 r.

Kongres poświęcony był problemom związanym z realizacją przepisów RODO oraz krajowych przepisów uzupełniających RODO. Pomimo iż wiele organizacji podjęło działania i wdrożyło rozwiązania formalne, organizacyjne i techniczne w celu zapewnienia przetwarzania danych osobowych zgodnie z przepisami, to jednak wciąż pojawiają się problemy na gruncie stosowania RODO w procesach przetwarzania danych przy użyciu nowych technologii, w szczególności w usługach internetowych. W panelu dyskusyjnym pt. „Główne problemy realizacji obowiązków RODO" uczestniczył Zastępca Prezesa UODO. Zagadnienia poruszone podczas tego panelu koncentrowały się na czterech podstawowych kwestiach związanych z bezpieczeństwem i ochroną danych osobowych w działalności IOD. A mianowicie: **współadministrowanie** (monitoring w budynkach, podczas organizacji konkursów,

w programach lojalnościowych, wspólnych platformach usługowych, rekrutacji, itd.), **udostępnianie danych a powierzenie ich przetwarzania** (wymogi RODO), **zwolnienia z obowiązku informacyjnego** (w oparciu o art. 14 RODO, oraz jak rozumieć „niewspółmiernie duży wysiłek", itd.), a także **przepisy dotyczące przetwarzania wizerunku** (analiza różnych przypadków).

20) Posiedzenie Zespołu ds. ETPCz. Warszawa, 10.12.2019 r.

Przedstawiciel Urzędu Ochrony Danych Osobowych uczestniczył w posiedzeniu Zespołu ds. Europejskiego Trybunału Praw Człowieka (ETPCz), zorganizowanym przez Ministerstwo Spraw Zagranicznych. Spotkanie, które odbyło się 10 grudnia 2019 r., prowadził Pełnomocnik RP przed ETPCz. Na początku spotkania przekazał on informacje na temat bieżącej działalności Zespołu w przedmiocie wykonywania wyroków ETPCz. Przedstawione zostały dostępne dane statystyczne za 2019 r. oraz informacje nt. posiedzeń grup roboczych Zespołu poświęconych wyrokom ETPCz przeciwko Polsce. Dodatkowo, Pełnomocnik RP przekazał informacje na temat wizyty studyjnej w Polsce przedstawicieli Biura Pełnomocnika Rządu Republiki Armenii przed ETPCz, a także informacje na temat ostatniego posiedzenia Komitetu Ministrów RE poświęconego nadzorowi nad wykonywaniem wyroków ETPCz (3-5.12.2019 r.) oraz informacje o planowanych na 2020 r. pracach Komitetu w tym zakresie. Spotkanie w MSZ stanowiło forum wymiany poglądów uczestników posiedzenia na temat działań podejmowanych na rzecz wykonywania wyroków ETPCz w 2019 r. i możliwych do podjęcia w 2020 r.

2. Działalność informacyjna

Działalność informacyjna UODO w minionym roku sprawozdawczym obejmowała obszerny i zróżnicowany zakres zagadnień tematycznych poświęconych ochronie danych osobowych. Działania te nie tylko koncentrowały się na informowaniu o bieżącej działalności organu nadzorczego. Wiele uwagi poświęcono także działaniom wspierającym uczestników systemu ochrony danych. Poza przybliżaniem administratorom i inspektorom ochrony danych zagadnień prawnych dotyczących stosowania RODO, Urząd Ochrony Danych Osobowych podejmował działania adresowane do szerszego grona odbiorców – osób indywidualnych, którym starano się przybliżyć przepisy RODO, biorąc pod uwagę zdarzenia, z którymi osoby te mogą mieć do czynienia na co dzień.

Generalnie działania informacyjne obejmowały: współpracę z przedstawicielami mediów, prowadzenie działań informacyjno-edukacyjnych poprzez media własne oraz obecność w mediach społecznościowych.

Do głównych działań w sferze informacyjnej podjętych przez UODO należały:

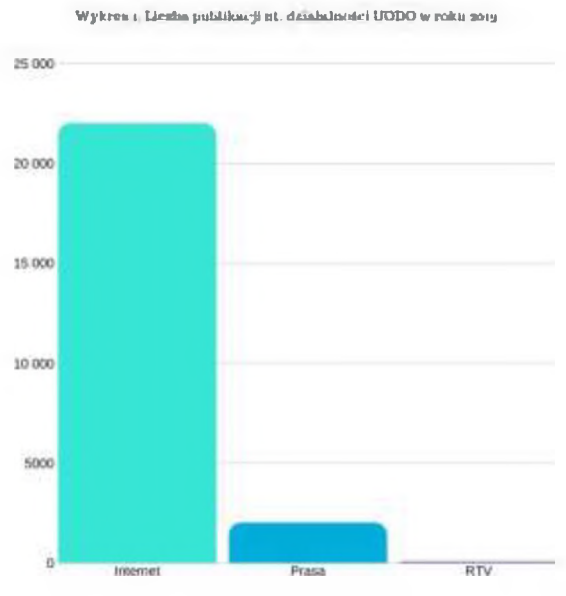
- organizacja spotkań z prasą w postaci briefingów prasowych,
- inicjowanie i redagowanie tekstów problemowych i poradnikowych udostępnianych na stronie www.uodo.gov.pl,
- udzielanie odpowiedzi na bieżące zapytania dziennikarzy mediów tradycyjnych i elektronicznych,
- aranżowanie wywiadów z ekspertami UODO,
- obsługa kanałów mediów społecznościowych Urzędu (Twitter w wersji polskiej i angielskiej, kanał na YouTube),
- promocja w mediach programu edukacyjnego „Twoje dane – Twoja sprawa" oraz projektów realizowanych przez UODO we współpracy z partnerami z zagranicy – „eOpenSpace", „T4DATA",
- wsparcie medialne eventów organizowanych przez Urząd lub z działem jego ekspertów, jak np. Dzień Ochrony Danych Osobowych,
- redakcja materiałów edukacyjnych Urzędu w postaci newslettera dla IOD,
- współtworzenie porad w publikacjach fachowych, itd.

2.1. Współpraca z mediami

W odniesieniu do stałej współpracy z mediami, to w porównaniu do roku ubiegłego (2018), nieznacznie wzrosła liczba opracowanych materiałów dla dziennikarzy, najczęściej w postaci informacji prasowych o tematyce ochrony danych. Przygotowano **123 tego typu opracowania**. Odbyło się **pięć briefingów prasowych**, a eksperci UODO udzielili mediom **75 wypowiedzi**, które w dużej mierze dotyczyły tematów lub były następstwem zdarzeń, wzbudzających największe zainteresowanie opinii publicznej.

W roku sprawozdawczym 2019 odnotowano w mediach więcej informacji nt. UODO niż rok wcześniej. W sumie w mediach tradycyjnych i na portalach internetowych ukazało się ponad **25 tys. wzmianek o Urzędzie Ochrony Danych Osobowych**. Dominowały wśród nich informacje dostępne w Internecie (przeszło 22 tys. wzmianek), a przeszło 2 tys. komunikatów opublikowano w prasie drukowanej. Eksperci UODO udzielili także blisko **60 wypowiedzi radiowo-telewizyjnych**. Do takiego stanu rzeczy przyczyniło się kilka elementów. Największą uwagę

dziennikarzy zwróciły zdarzenia, takie jak: zmiana na stanowisku Prezesa UODO, a także pierwsze decyzje Prezesa UODO o nałożeniu kar finansowych czy prowadzenie dwóch postępowań wobec Kancelarii Sejmu.



Wykres 13: Liczba publikacji w mediach na temat działalności UODO w 2019 r.

O ile w 2018 roku ogromnym zainteresowaniem dziennikarzy cieszyły się poradniki, to w roku sprawozdawczym 2019 ich miejsce zajęły opublikowane na stronie www.uodo.gov.pl **teksty problemowe i poradnikowe**, które zawierały wskazówki lub rekomendacje Prezesa UODO, jak należy stosować RODO na co dzień. Aktywność ta miała charakter akcji informacyjno-edukacyjnych, które w wielu przypadkach były inspirowane pytaniami kierowanymi do UODO od podmiotów z różnych środowisk i branż, w tym także od przedstawicieli mediów. Do opracowań najczęściej cytowanych w mediach należy wskazać artykuły poświęcone stanowisku Prezesa UODO w sprawie badania przez pracodawców stanu trzeźwości pracowników oraz działaniom zabezpieczającym przed utratą danych, w szczególności tym związanym z kradzieżą tożsamości.

Ponadto media szeroko informowały o obchodach 13. Dnia Ochrony Danych Osobowych, a także o zmianie struktury organizacyjnej Urzędu, której dodatkowo towarzyszyła zmiana logotypu.

Współpraca z mediami była prowadzona zarówno z prasą codzienną o zasięgu lokalnym i ogólnopolskim, ogólnopolskimi pismami branżowymi, a także objęła portale internetowe. Kontynuowana była również stała współpraca z ogólnopolskimi stacjami telewizyjnymi

i radiowymi o profilu informacyjnym oraz społeczno-gospodarczym. Regularna współpraca z czołowymi agencjami informacyjnymi zaowocowała realizacją wielu materiałów informacyjnych. W okresie sprawozdawczym rozwijano także współpracę w postaci publikacji cyklicznych materiałów eksperckich w czasopismach fachowych. Ponadto wybrane media obejmowały patronatem medialnym wydarzenia specjalne organizowane przez UODO, np. wspomniany 13. Dzień Ochrony Danych Osobowych oraz program edukacyjny „Twoje dane – Twoja sprawa".

2.2. Odpowiedzi na indywidualne pytania dziennikarzy

Szczególne miejsce w realizacji działań informacyjnych zajmuje udzielanie odpowiedzi na indywidualne pytania dziennikarzy. W roku sprawozdawczym 2019 odnotowano ponad **340 pytań** skierowanych do rzecznika prasowego Urzędu, tj. o 23 proc. więcej w stosunku do roku 2018.

Wśród zagadnień, którymi szczególnie interesowali się przedstawiciele mediów, podobnie jak w roku poprzednim, były m.in.:

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii,
- wykorzystywanie danych osobowych na potrzeby marketingu, ze szczególnym uwzględnieniem telemarketingu,
- udostępnianie nieznanym podmiotom – przez osoby, których dane dotyczą – szczegółowych informacji na swój temat, sposoby wyłudzania danych i zagrożenia z tym związane,
- żądanie pozostawienia dowodu osobistego lub innego dokumentu potwierdzającego tożsamość w zastaw za wypożyczony sprzęt sportowy oraz kopiowanie dokumentów tożsamości,
- odmowa udostępniania informacji publicznej, zwłaszcza przez jednostki samorządu terytorialnego, z powołaniem się na ochronę danych,
- możliwość stosowania monitoringu wizyjnego, np. przez pracodawców.

Z kolei jeśli chodzi o przepisy ogólnego rozporządzenia o ochronie danych, to dziennikarzy interesowało zwłaszcza:

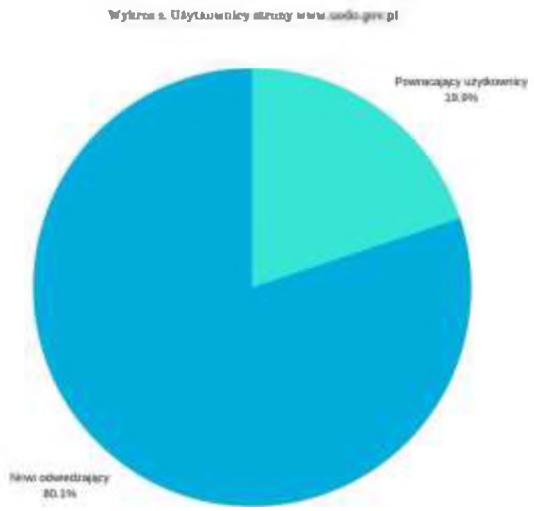
- liczba skarg, pytań oraz zgłoszonych naruszeń,
- nakładanie kar finansowych na administratorów łamiących zasady ochrony danych osobowych,
- reakcja UODO na wycieki danych,
- przetwarzanie danych osobowych w związku z organizacją wyborów, w procesie rekrutacji, przez szkoły oraz placówki zdrowia.

Dziennikarze interesowali się także naruszeniami ochrony danych. W wielu przypadkach śledzili postępy działań prowadzonych przez Prezesa UODO.

2.3. Strona internetowa i media społecznościowe

W 2019 roku Urząd Ochrony Danych Osobowych koncentrował się na rozwijaniu tzw. **mediów własnych**. Działania informacyjne były prowadzone głównie za pośrednictwem strony internetowej – www.uodo.gov.pl, na której regularnie publikowane były nowe oraz stale aktualizowane materiały, ważne dla uczestników systemu ochrony danych. W celu spełnienia oczekiwań jak największej liczby odbiorców, strona internetowa UODO została przebudowana – zredukowano liczbę zakładek tematycznych i usprawniono nawigację, co przyczyniło się do zwiększenia dostępności informacji najbardziej poszukiwanych. Na stronie internetowej Urzędu regularnie publikowane są decyzje Prezesa UODO. Zakładka z opublikowanymi decyzjami organu nadzorczego jest obecnie – obok zakładki „Aktualności" – najczęściej odwiedzaną częścią serwisu.

Co miesiąc odnotowuje się średnio ponad 350 tys. odsłon, co świadczy o dużym zainteresowaniu internautów informacjami dostarczanymi opinii publicznej poprzez witrynę internetową. W roku 2019 z zasobów strony skorzystało blisko 570 tys. użytkowników, w tym 80 proc. użytkowników to osoby, które zapoznały się z nią po raz pierwszy.



Wykres 14: Procentowy udział stałych i nowych użytkowników strony internetowej Urzędu Ochrony Danych Osobowych www.uodo.gov.pl

Ponadto w 2019 roku UODO wydawał cykliczny **newsletter dla inspektorów ochrony danych**. Uruchomiony w kwietniu 2019 roku biuletyn już na koniec analizowanego roku sprawozdawczego trafił do 6501 subskrybentów.

Istotnym wzmocnieniem wspomnianych działań informacyjnych w 2019 roku była systematyczna komunikacja prowadzona za pośrednictwem mediów społecznościowych – UODO prowadzi profile w serwisach Twitter oraz YouTube.

W przypadku profilu na **Twitterze** to liczba obserwujących przekroczyła już 3200 użytkowników i stale rośnie, a wzmianki o UODO pojawiły się ponad 3800 razy. W roku sprawozdawczym do grona obserwujących profil UODO na Twitterze dołączyło ponad 1200 nowych „followersów". Obserwujący profil 1166 razy udostępnili posty UODO, zaś łącznie – w całym 2019 roku – opublikowano ich 357.

Z kolei kanał UODO na **YouTube** odnotował ponad 115 tys. wyświetleń. Wśród dostępnych materiałów wideo rekordowe liczby odsłon odnotowały nagrania poświęcone profilaktyce w zakresie ochrony danych, np. film pt. „W oku kamery. Monitoring wizyjny", który wyświetlono ponad 7 tys. razy.

2.4. Infolinia

Na dwa i pół miesiąca przed rozpoczęciem stosowania RODO, 12 marca 2018 r. w Urzędzie Ochrony Danych Osobowych uruchomiona została infolinia, którą na koniec 2019 r. obsługiwało siedmiu pracowników.

Pracownicy infolinii posiadają wiedzę z zakresu ochrony danych osobowych, którą systematycznie uzupełniają, uczestnicząc w specjalistycznych szkoleniach oraz monitorując aktualny stan prawny – w tym orzecznictwo krajowe i europejskie – oraz wydane przez Prezesa UODO decyzje administracyjne. W zakresie udzielanych porad prawnych współpracują z innymi departamentami UODO, korzystając z ich merytorycznego wsparcia. Przekazują informacje o postępach w zainicjowanych przed Urzędem postępowaniach skargowych, procedurze składania skarg i wniosków, prawidłowym wypełnianiu i przesyłaniu formularzy zgłoszeń naruszeń oraz zgłoszeń powołania, odwołania i innych zmian w odniesieniu do Inspektora Ochrony Danych, a także o wydarzeniach z dziedziny ochrony danych osobowych, w tym o szkoleniach i konferencjach organizowanych lub współorganizowanych przez UODO. Eksperci obsługujący infolinię wskazują konkretne miejsca na stronie internetowej Urzędu lub Europejskiej Rady Ochrony Danych, gdzie można znaleźć wytyczne i wskazówki z zakresu ochrony danych osobowych. Poprzez infolinię przekazywane są nie tylko informacje związane z działalnością Urzędu, ale także zbierane są informacje komunikowane przez osoby telefonujące do UODO na temat problemów, którymi w ich opinii powinien zająć się organ właściwy w sprawach ochrony danych osobowych.

Tematyka przeprowadzonych rozmów była bardzo różnorodna. Najczęściej zadawane pytania dotyczyły (oprócz pytań w kwestii stanu sprawy toczącej się w Urzędzie) następujących zagadnień: wyciek danych w Virgin Mobile, podawanie nr PESEL w punktach sprzedaży węgla czy na kopercie z życzeniami świątecznymi, legalność kserowania/skanowania dowodów osobistych, niechciany telemarketing, przetwarzanie danych osobowych przez pracodawców czy firmy windykacyjne, wyczytywanie pełnych danych z numerem telefonu w poczekalni u weterynarza, mail z urzędu z odkrytą listą mailingową, różnica między administratorem, współadministratorem i podmiotem przetwarzającym, zasadność zbierania przez szkoły danych uczniów na rzecz gabinetów dentystycznych, z którymi podpisano umowy na opiekę dentystyczną w szkołach, czy skarbnik gminy ma prawo wglądu do dokumentacji ZFŚS, co zrobić z dokumentacją ZFŚS zebraną pod rządami ustawy sprzed nowelizacji, czy audytor wewnętrzny potrzebuje upoważnienia do przetwarzania danych osobowych, podstawa prawna nagrywania rozmów telefonicznych i wiele innych.

Niemniej jednak można wskazać podstawowe kategorie spraw, których zadawane pytania dotyczyły: zakres stosowania i obowiązki wynikające z ogólnego rozporządzenia o ochronie danych, RODO a inne akty prawne, zasady i podstawy przetwarzania danych, obowiązek informacyjny, dokumentacja związana z przetwarzaniem danych osobowych, prawa przysługujące osobom fizycznym w związku z przetwarzaniem ich danych, umowy powierzenia i relacje administrator – podmiot przetwarzający, reguły korporacyjne i przekazywanie danych do państw trzecich, obowiązek wyznaczenia inspektora ochrony danych osobowych, jego zadania i status, obowiązki administratora związane z naruszeniami ochrony danych osobowych i sposób zgłaszania naruszeń, praca UODO oraz sposób składania skarg, zawiadomienia Prezesa UODO związane z wyznaczeniem IOD, wyznaczanie IOD na podstawie ustawy o ochronie danych osobowych, jak i z ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Rozmowy najczęściej dotyczyły spraw sąsiedzkich, konsumenckich, kadrowych, szkoleń, rekrutacji, służby zdrowia, szkolnictwa, pomocy społecznej, monitoringu oraz prowadzenia działalności gospodarczej, obejmując tematykę różnych branż, np. telekomunikacyjnej, budowlanej, transportowej, usługowej czy handlu elektronicznego.

Techniczne uwarunkowania infolinii nie pozwalają na przedstawienie dokładnej liczby odebranych połączeń. Trzeba mieć też na uwadze, że jedno połączenie, to często kilka pytań od tej

samej osoby, często dotyczących różnych zagadnień. Niemniej warto podkreślić, że w 2019 roku siedmioosobowy skład infolinii przeprowadził około 29 000 konsultacji.

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 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 Prezesa Urzędu prowadzonych w ramach współpracy międzynarodowej należał udział w posiedzeniach Europejskiej Rady Ochrony Danych, w tym w pracach podgrup tematycznych, udział w pracach Komitetu Konsultacyjnego Rady Europy, współpraca z rzecznikami ochrony danych innych krajów – w szczególności w ramach Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, której jest założycielem i w której pełni rolę Sekretariatu, oraz udział w organizowanych cyklicznie Międzynarodowych Konferencjach Rzeczników Ochrony Danych i Prywatności, Wiosennych Konferencjach Europejskich Organów Ochrony Danych oraz w Warsztatach Rozpatrywania Spraw.

Podkreślenia wymaga, że ww. Wiosenne Konferencje są najważniejszym, corocznym spotkaniem wszystkich rzeczników ochrony danych osobowych z państw członkowskich UE, innych państw europejskich oraz przedstawicieli Komisji Europejskiej, Rady Europy oraz innych organów zajmujących się ochroną danych osobowych. Poszczególne konferencje poświęcone są różnym aspektom ochrony danych osobowych w Europie, a ich uczestnicy podejmują działania ukierunkowane nie tylko na wdrażanie unijnych przepisów, ale również na monitorowanie ich przestrzegania w poszczególnych krajach.

Inne ważne zadania stojące przed polskim organem ds. ochrony danych w ramach współpracy międzynarodowej, związane są z jego udziałem w pracach grup koordynujących nadzór nad SIS II, VIS, CIS, IMI, Eurodac, Wspólnego Organu Nadzorczego nad Systemem Informacji Celnej (CIS), a także Rady Współpracy Europolu.

W ramach współpracy międzynarodowej z organami nadzorczymi innych państw członkowskich UE oraz wykonywania obowiązków wynikających z członkostwa Polski w Unii Europejskiej, UODO przygotowywał informacje mające znaczenie dla stanowiska Polski w sprawach dotyczących ochrony danych osobowych, stanowiących przedmiot postępowań prowadzonych przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE). Informacje te stanowiły część materiału wyjściowego do udzielanych przez stosowny organ ze strony Polski, odpowiedzi na pytania prejudycjalne TSUE.

1. Europejska Rada Ochrony Danych - EROD

Od 25 maja 2018 r. Urząd Ochrony Danych Osobowych wchodzi w skład Europejskiej Rady Ochrony Danych (EROD), która została ustanowiona ogólnym rozporządzeniem o ochronie danych (RODO)[241], zastępując Grupę Roboczą Artykułu 29, powołaną na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, jako niezależny podmiot o charakterze doradczym.

EROD jako organ Unii posiada osobowość prawną. W jej skład wchodzą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych (EIOD) lub ich przedstawiciele. Podkreślenia wymaga, że 26 listopada 2019 r. Europejskim Inspektorem Ochrony Danych na 5-letnią kadencję wybrany został dr Wojciech R. Wiewiórowski, który w latach 2010- 2014 pełnił funkcję polskiego organu ds. ochrony danych osobowych.

Komisja Europejska ma prawo udziału w działaniach i posiedzeniach EROD, nie ma jednak prawa głosu. Radę reprezentuje jej przewodniczący. 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 Urzędu Ochrony Danych Osobowych lub jego przedstawiciel uczestniczyli w odbywających się co miesiąc w Brukseli posiedzeniach plenarnych Europejskiej Rady Ochrony

[241] EROD została ustanowiona na mocy art. 68 ust. 1 RODO.

Danych. Udział ten miał kluczowe znaczenie nie tylko z punktu widzenia przestrzegania mechanizmu spójności i współpracy, o którym jest mowa w rozdziale VII RODO, ale również, jak potwierdza doświadczenie pierwszego roku stosowania RODO, z punktu widzenia wypracowywania stanowisk spójnych z europejskimi wytycznymi, 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 Urzędu Ochrony Danych Osobowych w posiedzeniach plenarnych EROD uznać należy za niezwykle istotny[242].

Zgodnie z art. 29 regulaminu wewnętrznego Rady, w lutym 2019 roku EROD przyjęła dwuletni program prac na lata 2019–2020. Program prac EROD jest oparty na potrzebach określonych przez członków jako priorytetowe dla osób fizycznych i zainteresowanych stron, a także na działaniach zaplanowanych przez unijnego prawodawcę.

Zgodnie z ustalonym planem, w 2019 roku Rada roku przyjęła następujące dokumenty:

1) Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679;
2) Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą;
3) Rekomendacje 1/2019 w sprawie wykazu Europejskiego Inspektora Ochrony Danych rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (art. 39 ust. 4 Rozporządzenia (UE) 2018/1725);
4) Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo;
5) Wytyczne 4/2019 w sprawie art. 25 RODO poświęcone ochronie danych w fazie projektowania oraz domyślnej ochronie danych;
6) Wytyczne 5/2019 w sprawie kryteriów dotyczących prawa do bycia zapomnianym w wyszukiwarkach internetowych na mocy RODO (część 1).

[242] Więcej szczegółowych informacji na temat dyskutowanych podczas posiedzeń EROD kwestii, znajduje się na stornie internetowej UODO https://uodo.gov.pl/pl/p/posiedzenia-plenarne-erod

2. 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 Urzędu Ochrony Danych Osobowych, którzy reprezentują polski organ nadzorczy w 13 grupach:

- Podgrupa ds. Kluczowych Przepisów (Key Provisions Expert Subgroup),
- Podgrupa ds. Użytkowników IT (IT Users Expert Subgroup),
- Podgrupa ds. Technologii (Technology Expert Subgroup),
- Podgrupa ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS),
- Podgrupa ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health - CEH),
- Podgrupa ds. Współpracy (Cooperation Expert Subgroup),
- Podgrupa ds. Nakładania Kar (Fining Task Force),
- Podgrupa ds. Sektora Finansowego (Financial Matters Expert Subgroup),
- Podgrupa ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup - BTLE),
- Podgrupa ds. Egzekwowania Prawa (Enforcement Expert Subgroup),
- Podgrupa ds. Mediów Społecznościowych (Social Media Expert Subgroup),
- Podgrupa ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS), a także:
- Podgrupa Ekspercka ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup - SAS).

Pracownicy Urzędu Ochrony Danych Osobowych biorą aktywny udział w pracach podgrup eksperckich Rady, angażując się w działania związane m.in. z rozwijaniem wykładni przepisów, współpracą między organami nadzorczymi oraz podejmowaniem bieżących problemów związanych z ochroną danych osobowych w związku z rozwojem nowoczesnych technologii. Podczas tych spotkań omawiają kwestie prawne i techniczne związane z funkcjonowaniem systemów informatycznych SIS II, VIS, EURODAC oraz przetwarzaniem danych przez EUROPOL. Uczestniczą w ewaluacjach dotyczących funkcjonowania systemu SIS II i VIS, odbywających się zarówno w Polsce, jak i w innych państwach UE, a w szczególności w pracach grupy eksperckiej

BTLE zajmującej się kwestią transgranicznego transferu i przetwarzaniem danych osobowych przez organy ścigania. Opracowują opinie, wytyczne, zalecenia i najlepsze praktyki w celu promowania wspólnej wykładni przepisów RODO i dyrektywy 2016/680 (tzw. dyrektywy policyjnej), a także doradzają Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych w UE. Dokumenty te są następnie przedmiotem dyskusji, by w końcu zostały przyjęte podczas comiesięcznych posiedzeń plenarnych EROD.

3. Współpraca UODO z innymi organami nadzorczymi

Organy nadzorcze, jak stanowi motyw 133 RODO, powinny się wzajemnie wspierać w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie rozporządzenia na rynku wewnętrznym. Na podstawie art. 61 ust. 1 RODO, organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania RODO oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i przeprowadzenie uprzednich konsultacji oraz o przeprowadzenie kontroli i postępowań wyjaśniających. Zgodnie natomiast z art. 56 ust. 1 RODO w przypadku transgranicznego przetwarzania danych, dokonywanego przez administratora lub podmiot przetwarzający, organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy – zgodnie z procedurą przewidzianą w art. 60 RODO.

Temu celowi służy system IMI – bezpieczny, wielojęzyczny serwis internetowy, który umożliwia wymianę informacji organom publicznym zaangażowanym we wdrażanie przepisów unijnych. Opracowano go z myślą o usprawnieniu wymiany informacji między organami administracji publicznej w EOG i europejskimi instytucjami i organami zaangażowanymi w praktyczne wdrażanie prawa Unii. IMI pomaga organom państwowym w wypełnianiu obowiązków z zakresu współpracy międzynarodowej w wielu dziedzinach związanych z jednolitym rynkiem. Dzięki IMI udało się unowocześnić współpracę administracyjną w skali międzynarodowej i zapewnić sprawne funkcjonowanie jednolitego rynku. Choć użytkownikami końcowymi IMI są krajowe organy publiczne, beneficjentami sprawniejszej współpracy są firmy i konsumenci.

Urząd Ochrony Danych osobowych korzysta z IMI, jako narzędzia wymiany informacji pomiędzy organami nadzorczymi państw członkowskich.

System IMI umożliwia realizację procedur współpracy i spójności, o których mowa w Rozdziale VII RODO, w tym wdrażanie poniższych przepisów RODO:

- Artykuł 56 – właściwość wiodącego organu nadzorczego,
- Artykuł 60 – współpraca miedzy wiodącym organem nadzorczym (LSA) a innymi organami nadzorczymi, których sprawa dotyczy (CSA),
- Artykuł 61 – wzajemna pomoc,
- Artykuł 62 – wspólne operacje organów nadzorczych,
- Artykuł 64 – opinia EROD,
- Artykuł 65 – rozstrzyganie sporów przez EROD,
- Artykuł 66 – tryb pilny.

Zgodnie z przygotowanymi przez Helpdesk IMI statystykami, według stanu na dzień 31 grudnia 2019 r. w rejestrze spraw IMI znajdowało się **807** spraw dotyczących współpracy transgranicznej.

Podział tych spraw znajduje się poniżej:

- w wyniku skarg wszczęto **575** spraw;
- **232** sprawy pochodzą z innych źródeł, takich jak postępowanie przygotowawcze, inicjatywa organu nadzorczego, zobowiązanie prawne, ocena skutków dla ochrony danych, itp.

Z powyższych spraw uruchomiono następujące procedury:

- **2427** procedur dotyczących Wzajemnej Pomocy (art. 61). Procedury te mogą w przyszłości prowadzić do uruchomienia mechanizmów One-stop-shop;
- **497** procedur One-stop-shop (art. 60), z których: 74 stanowią Decyzję Ostateczną, 131 Projekt Decyzji, 17 Zmieniony Projekt Decyzji i 246 Nieformalne Konsultacje;
- **65** Wniosków w sprawach lokalnych (art. 56 ust. 2);
- Procedury spójności: **48** procedur określonych w art. 64.

Jednym z zadań Prezesa Urzędu Ochrony Danych Osobowych jest prowadzenie, a także uczestniczenie w postępowaniach prowadzonych przez inne organy nadzorcze, jeżeli dotyczą one transgranicznego przetwarzania. W 2019 r. przeważająca liczba takich postępowań dotyczyła podmiotów sektora prywatnego. Zgodnie z art. 4 pkt 23 RODO „transgraniczne przetwarzanie" oznacza „przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub

podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim". W przypadku gdy sprawa ma charakter transgraniczny, zostaje – zgodnie z art. 56 ust. 1 RODO – przekazana wiodącemu organowi nadzorczemu, a zgodnie z art. 60 RODO organy, których sprawa dotyczy (art. 4 pkt 22 RODO) przyłączają się do postępowania. Przyłączenie do postępowania w charakterze organu, którego sprawa dotyczy, pozwala na etapie wydawania decyzji, na zaopiniowanie projektu decyzji, a także na zgłoszenie uzasadnionego sprzeciwu co do jej treści. Ewentualnie w sytuacji konfliktu, możliwym jest wystosowanie wniosku o wydanie wiążącej decyzji przez Europejską Radę Ochrony Danych na podstawie art. 65 ust. 1 RODO.

W 2019 r. Urząd zgłosił gotowość przystąpienia do postępowań transgranicznych w charakterze organu, którego sprawa dotyczy w **219 sprawach**. Natomiast nie zgłaszał takiej gotowości w odniesieniu do tych postępowań transgranicznych, które w jego ocenie miały charakter lokalny – nie dotyczyły ani jednostek organizacyjnych administratora znajdujących się na terytorium Polski, ani też w znaczny sposób nie wpływały na osoby, których dane dotyczą rezydujące w Polsce[243].

Jak już wspomniano wyżej, najwięcej skarg dotyczących przetwarzania transgranicznego, które wpłynęły w 2019 r. do **systemu wymiany informacji pomiędzy organami nadzorczymi**[244] **(IMI)** związanych było z działalnością podmiotów sektora prywatnego: portali społecznościowych, platform sprzedażowych oraz platform umożliwiających płatności on-line, banków, linii lotniczych oraz pośredników w rezerwacji miejsc noclegowych. W sprawach podmiotów sektora prywatnego Prezes UODO przekazał **17 spraw**, które do niego wpłynęły, wiodącym organom nadzorczym, wydał **16 decyzji** w postępowaniach dotyczących przetwarzania transgranicznego, dla których był organem, którego sprawa dotyczyła.

---

[243] Charakter lokalny przetwarzania transgranicznego można stwierdzić, jeżeli sprawa dotyczy wyłącznie jednostki organizacyjnej w jednym państwie członkowskim lub znacznie wpływa na osoby, których dane dotyczą, wyłącznie w jednym państwie członkowskim (zob. art. 56 ust. 2 rozporządzenia 2016/679).

[244] System wymiany informacji pomiędzy organami nadzorczymi, system IMI, został wdrożony jako projekt pilotażowy decyzją wykonawczą KE, zob. DECYZJA WYKONAWCZA KOMISJI (UE) 2018/743 z dnia 16 maja 2018 r. w sprawie projektu pilotażowego mającego na celu wdrożenie przepisów o współpracy administracyjnej określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679, za pomocą systemu wymiany informacji na rynku wewnętrznym. System ten ułatwia komunikację między organami nadzorczymi, a także zapewnia jej poufność.

Wskazać należy, że w stosunku do ubiegłego roku, w analizowanym 2019 roku czterokrotnie wzrosła liczba spraw, dla których Prezes UODO był organem wiodącym, gdyż w 2018 r. Prezes UODO prowadził tylko jedno postępowanie jako organ wiodący. Ponadto ponad dwukrotnie wzrosła liczba postępowań w sprawach, dla których Prezes UODO zidentyfikował się jako organ, którego sprawa dotyczy, gdyż w przeważającej mierze albo administrator posiadał jednostkę organizacyjną na terytorium Polski albo przetwarzanie mogło mieć wpływ na osoby rezydujące na terytorium Polski. **W 2018 r. Prezes UODO zgłosił chęć przystąpienia do postępowania jako organ, którego sprawa dotyczy w 110 postępowaniach, zaś w 2019 r. takich sytuacji odnotowano 219.**

Podobnie jak w minionym roku sprawozdawczym, również w 2019 roku skargi dotyczyły przetwarzania transgranicznego administratorów, których działalność miała zasięg europejski lub światowy. Zmniejszyła się jednakże liczba skarg na operatorów wyszukiwarek internetowych, gdyż większość z nich posiadała główną jednostkę organizacyjną poza obszarem EOG i sprawy ich dotyczące prowadzone były na szczeblu krajowym. Działo się tak dlatego, że mechanizm prowadzenia spraw transgranicznych przy wykorzystaniu mechanizmu z art. 60 tzw. „mechanizmu OSS" (ang. *One-stop-shop*) nie odnosi się do prowadzonego przez te wyszukiwarki przetwarzania danych osobowych.

W 2019 r. w sprawach dotyczących podmiotów sektora prywatnego Urząd wszczął **cztery postępowania, w którym Prezes Urzędu Ochrony Danych Osobowych został wskazany jako organ wiodący.** Skargi prowadzone przez polski organ nadzorczy jako organ wiodący dotyczyły administratorów przetwarzających dane w związku z oferowaniem usług: książki telefonicznej on-line, pośrednictwa pracy, bankowych oraz przewozów lotniczych. Jedno z tych postępowań zostało zidentyfikowane jako mające charakter lokalny i prowadzone było przez czeski organ nadzorczy. W analizowanym okresie sprawozdawczym rozpoznanych zostało (w tym utworzonych) ponad 500 wniosków dotyczących wszczęcia postępowań transgranicznych przekazanych przez system IMI.

W analizowanym 2019 roku, w wyniku współpracy organów nadzorczych działających na rynku wewnętrznym, w odniesieniu do spraw sektora zdrowia, zatrudnienia i szkolnictwa prowadzone były łącznie **52 postępowania**, co stanowi znaczny wzrost w porównaniu z poprzednim rokiem sprawozdawczym, w którym prowadzono łącznie 6 postępowań. Powyższy wzrost świadczy o wzmożeniu wzajemnej współpracy organów nadzorczych w tym obszarze, co w dalszej perspektywie wzmocni efektywność ich działań i przyczyni się do zwiększenia efektywności w zapewnieniu spójnego stosowania i egzekwowania RODO na rynku wewnętrznym.

Spośród powyższych 52 postępowań **16 prowadzono w trybie art. 56 RODO**, przy czym w żadnym z ww. postępowań nie uznano, że wiodącym organem nadzorczym jest Prezes UODO. **W trybie art. 61 RODO prowadzono natomiast 36 postępowań**, z których 31 postępowań zainicjowanych zostało przez polski organ nadzorczy, zaś 5 postępowań zainicjowanych zostało przez organy nadzorcze innych państw.

Podkreślenia wymaga, że współpraca pomiędzy organami nadzorczymi jest zacieśniania w ramach prac Podgrup Cooperation oraz Enforcement działających w ramach Europejskiej Rady Ochrony Danych, podczas których omawiane są problemy związane z m.in. prowadzeniem postępowań transgranicznych. Wraz z zaangażowaniem pracowników Urzędu w prace Europejskiej Rady Ochrony Danych, wzrasta rola i rozpoznawalność polskiego organu nadzorczego na arenie europejskiej i międzynarodowej.

4. Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy

W analizowanym 2019 r. do Urzędu Ochrony Danych Osobowych wpływały – w ramach procedury określonej w dokumencie Grupy Roboczej Art. 29 WP 263 rev. 01 „Working Document Setting Forth a Co-Operation Procedure for the approval of „Binding Corporate Rules" for controllers and processors under the GDPR" („dokument WP 263") – zapytania od organów nadzorczych z Europejskiego Obszaru Gospodarczego (EOG) dotyczące wiążących reguł korporacyjnych (WRK) w ponad 50 różnych grupach kapitałowych.

Zapytania te najczęściej dotyczyły zgłoszenia ewentualnych zastrzeżeń odnośnie ustanowienia w ramach danej procedury zatwierdzania WRK organu wiodącego, ewentualnych komentarzy do projektu konkretnych wiążących reguł korporacyjnych (ich skonsolidowanego projektu, będącego rezultatem współpracy organu wiodącego i współsprawozdawców), czy ewentualnych komentarzy do projektu konkretnych WRK przesyłanych do wszystkich członków podgrupy EROD – International Transfers Subgroup („ITS"), które następnie były dyskutowane podczas specjalnych sesji dotyczących WRK, odbywających się bezpośrednio po posiedzeniu podgrupy ITS. Obecnie grupy mają możliwość ubiegania o zatwierdzenie dwóch rodzajów wiążących reguł korporacyjnych, tj. wiążących reguł korporacyjnych dla administratorów (Binding Corporate Rules for Controllers, BCR-C) oraz wiążących reguł korporacyjnych dla podmiotów przetwarzających (Binding Corporate Rules for Processors, BCR-P), więc zapytania te dotyczyły obu rodzajów WRK. Powyższa nieformalna współpraca odbywa się obecnie z uwzględnieniem mechanizmu spójności przewidzianego w art. 63 RODO, przy współpracy z innymi organami nadzorczymi UE, po zasięgnięciu opinii Europejskiej Rady Ochrony Danych. Formalne

zatwierdzenie wiążących reguł korporacyjnych poprzedza wspomniana nieformalna współpraca organów nadzorczych określona w dokumencie WP 263. Na początku procedury współpracy konieczne jest ustalenie tzw. organu wiodącego, który będzie właściwy do wydania decyzji zatwierdzającej wiążące reguły korporacyjne i który będzie swego rodzaju punktem kontaktowym zarówno dla grupy wnioskującej o zatwierdzenie przedmiotowych reguł, jak i dla innych organów nadzorczych z Europejskiego Obszaru Gospodarczego w ramach wspomnianej procedury nieformalnej współpracy (pkt. 1.2 dokumentu WP 263).

Po przeprowadzeniu przez organ wiodący wstępnej, pierwszej oceny przedłożonego przez grupę projektu wiążących reguł korporacyjnych, przedmiotowy projekt jest następnie przesyłany organowi nadzorczemu / organom nadzorczym działającym w danej sprawie jako tzw. współ-recenzenci (tzw. co-reviewerzy). Ich liczba zależy od ilości tzw. zainteresowanych organów nadzorczych, tj. organów nadzorczych z państw UE, z których będą przekazywane dane osobowe do podmiotów z danej grupy kapitałowej, zlokalizowanych w państwach trzecich. Dopiero gdy organ wiodący we współpracy z tzw. co-reviewerami uzna, że wstępny, pierwszy projekt wiążących reguł korporacyjnych, przedłożony przez grupę kapitałową, w ocenie wskazanych organów nadzorczych spełnia wymogi przewidziane dla wiążących reguł korporacyjnych i może zostać zakwalifikowany jako tzw. projekt skonsolidowany (ang. consolidated draft), organ wiodący przesyła przedmiotowy projekt do wszystkich zainteresowanych organów nadzorczych z EOG. Uzgodniono również, że przed formalnym przedłożeniem do EROD (z prośbą o wydanie opinii) projektu decyzji zatwierdzającej konkretne WRK, rozpatrywane WRK są jeszcze przedmiotem specjalnej sesji poświęconej WRK, odbywającej się po **posiedzeniu podgrupy ITS.** W analizowanym 2019 r. polski organ nadzorczy działał jako organ wiodący w rozumieniu wspomnianej wyżej procedury współpracy w jednej sprawie dotyczącej zatwierdzenia WRK w jednej grupie kapitałowej.

Na uwagę zasługuje wniosek Komisji Nadzoru Finansowego, który wpłynął do UODO 14.05.2019 r. o udzielenie zezwolenia na uzgodnienie administracyjne w sprawie przekazywania danych osobowych między Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych – ESMA i krajowymi organami ds. regulacji papierów wartościowych i rynków z Europejskiego Obszaru Gospodarczego z jednej strony a organami ds. regulacji papierów wartościowych i rynków z państw trzecich z drugiej strony. W dniu 22 listopada 2019 r. została wydana decyzja, w której Prezes UODO udzielił zezwolenia na postanowienia przedłożonego uzgodnienia administracyjnego. Nakazał ponadto Komisji Nadzoru Finansowego informowanie Prezesa Urzędu Ochrony Danych Osobowych, bez nieuzasadnionej zwłoki, o każdym zawieszeniu przekazywania danych osobowych

na podstawie pkt III ppkt 8 i pkt IV Uzgodnienia administracyjnego oraz o każdym przeglądzie Uzgodnienia administracyjnego i zakończeniu uczestnictwa w Uzgodnieniu administracyjnym stosownie do postanowień jego pkt V[245].

Tematyka innych zapytań prawnych, dotyczących różnych aspektów związanych z przekazywaniem danych osobowych do państw trzecich, dotyczyła m.in. procedury zatwierdzania wiążących reguł korporacyjnych oraz czasu jej trwania, przekazywania danych osobowych do podmiotu w Stanach Zjednoczonych, który nie jest objęty programem samo certyfikacji Privacy Shield, a także kwestii związanych z możliwością skutecznej ochrony danych osobowych.

5. Wizyty robocze

Wizyta Profesora Dietera Kugelmanna w UODO. Warszawa, 1-5.07.2019 r.

W dniach 1-5 lipca 2019 r. w Urzędzie Ochrony Danych Osobowych przebywał w ramach wizyty ***work shadowing*** Prof. dr Dieter Kugelmann, który od 1 października 2015 r. pełni funkcję Rzecznika Ochrony Danych i Wolności Informacji Kraju Związkowego Nadrenia-Palatynat. Celem wizyty było uzyskanie wglądu w struktury i metody pracy UODO oraz wymiana wspólnych doświadczeń obu urzędów. Największe zainteresowanie Profesora budziły kwestie związane ze skargami oraz naruszeniami ochrony danych, funkcjonowanie sytemu IMI, ochrona danych osobowych w mediach, kościołach oraz wyłączenia z RODO. Wśród innych zagadnień znalazły się także kary nakładane przez Prezesa UODO, środki naprawcze oraz prace przedstawicieli UODO w grupach eksperckich działających w ramach EROD. W ramach tej wizyty odbyło się również spotkanie Profesora D. Kugelmanna ze Związkiem Banków Polskich, dotyczące kodeksów postępowania.

Wizyta studyjna przedstawicieli białoruskich organów publicznych w siedzibie UODO. Warszawa, 16-17.10.2019 r.

Narodowe Centrum Legislacji i Badań Prawnych Republiki Białorusi przygotowuje projekt ustawy o ochronie danych osobowych oraz ramy funkcjonowania przyszłego organu nadzorczego w tym kraju. Rada Europy, która w ramach programu współpracy, udziela wsparcia Republice Białorusi w opracowaniu jej przyszłego prawa dotyczącego ochrony danych osobowych, zaproponowała zorganizowanie wizyty studyjnej przedstawicieli białoruskich organów publicznych w siedzibie polskiego Urzędu Ochrony Danych Osobowych. Przedmiotowe spotkanie odbyło się

[245] Przedmiotowa decyzja wydana w 2019 r. jest ostateczna, ale nieprawomocna.

w dniach 16-17 października 2019 r. z udziałem 8 przedstawicieli białoruskich organów i instytucji publicznych Zgromadzenia Narodowego Republiki Białorusi, administracji prezydenta i administracji rządowej oraz urzędu statystycznego. Spotkanie to zorganizowane zostało w ramach programu „Poprawa ochrony danych w Republice Białorusi" realizowanego przez Radę Europy. Podczas wizyty przedstawiciele Urzędu Ochrony Danych Osobowych przybliżyli delegacji białoruskiej funkcjonowanie polskiego organu nadzorczego, zasady wynikające z ogólnego rozporządzenia o ochronie danych oraz rolę inspektorów ochrony danych i ich zadania.

Dwudniowa wizyta studyjna delegacji białoruskiej w Polsce była kontynuacją spotkania, które odbyło się w siedzibie Rady Europy w Strasburgu w maju 2019 r. Wówczas delegacja białoruska miała okazję zapoznać się z Konwencją 108 oraz międzynarodowymi standardami ochrony danych osobowych, orzecznictwem Europejskiego Trybunału Praw Człowieka oraz procedurami przystąpienia do traktatu[246].

6. Międzynarodowe Warsztaty

1) Warsztaty EIOD dotyczące wyborów. Bruksela, 1.02.2019 r.

W marcu 2018 r. Europejski Inspektor Ochrony Danych wydał opinię w sprawie manipulacji online i ochrony danych (Opinia 3/2018)[247], w której zidentyfikowano potrzebę ułatwienia rozmów na temat niewłaściwego wykorzystywania danych osobowych w związku z wyborami i jego wpływu na demokratyczne wybory, między organami ochrony danych a organami odpowiedzialnymi za regulację kwestii związanych z wyborami.

W świetle wyborów w Parlamencie Europejskim w maju 2019 r. oraz wyborów zaplanowanych w wielu krajach na rok 2019, Europejski Inspektor Ochrony Danych zorganizował jednodniowe warsztaty poświęcone tej kwestii. Najważniejszymi celami tych warsztatów było umiejscowienie organów ochrony danych w centrum debaty dotyczącej ochrony danych osobowych w trakcie kampanii wyborczej. Dla organizatora tego wydarzenia istotne było stworzenie przestrzeni, w której organy ochrony danych, organy odpowiedzialne za regulację kwestii związanych z wyborami oraz organy regulujące kwestie usług audiowizualnych – mogłyby wskazać potencjalne słabe strony, doświadczenia i luki w zakresie kompetencji oraz znaleźć praktyczne sposoby zajęcia się kwestią niewłaściwego wykorzystywania danych osobowych oraz manipulacji

[246] Więcej informacji o projekcie Rady Europy, zob. link: https://www.coe.int/en/web/data-protection/enhancing-data-protection-belarus
[247] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

w związku z wyborami. Oprócz zagadnień związanych z ochroną danych osobowych w trakcie prowadzenia kampanii wyborczej, dyskutowano też na temat roli portali społecznościowych.

2) Warsztaty Rozpatrywania Spraw. Bruksela, 28-29.11.2019 r.

Przedstawiciel UODO uczestniczył w corocznych warsztatach rozpatrywania spraw. W roku 2019 odbywały się one w Brukseli. Tematyka tegorocznych warsztatów dotyczyła zagadnień związanych m.in. z takimi kwestiami, jak:

– zawieranie umów na użycie informatycznych rozwiązań przez instytucje publiczne,

– prowadzenie spraw transgranicznych lokalnie – tj. za zgodą organu wiodącego (właściwość delegacyjna) – i wynikające z tego problemy w sytuacji odmowy współpracy przez jednostkę organizacyjną administratora, mającą siedzibę w państwie organu właściwego lokalnie,

– stosowanie uprzednich konsultacji, zwłaszcza gdy ryzyka (negatywne efekty) przeważają nad możliwością ich eliminacji, oraz co należy przygotować przed uprzednią konsultacją,

– ochroną „sygnalistów" zgłaszających organowi nadzorczemu naruszenie ochrony danych,

– działalność podmiotów sprawdzających zdolność kredytową.

7. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2019 r. Prezes UODO i jego przedstawiciele uczestniczyli w konferencjach, seminariach i spotkaniach o charakterze międzynarodowym w kraju i za granicą.

Wykaz wydarzeń o charakterze międzynarodowym, które odbyły się w 2019 r. z udziałem Prezesa UODO lub jego przedstawicieli znajduje się w załączniku nr 4. Poniżej przedstawione zostały wybrane przykłady najważniejszych wydarzeń.

1) Konferencja nt. wpływu rozwoju sztucznej inteligencji na prawa człowieka, demokrację i praworządność. Helsinki, 26-27.02.2019 r.

Konferencja pt. „Governing the Game Changer – Impacts of artificial intelligence development on human rights, democracy and the rule of law", współorganizowana przez Fińską Prezydencję Komitetu Ministrów Rady Europy i Radę Europy, odbyła się w dniach 26-27 lutego 2019 r. w Helsinkach w Finlandii. Jej celem było podjęcie krytycznej, otwartej i pluralistycznej debaty na temat tego, jak odnieść się do rozwoju sztucznej inteligencji, aby zmaksymalizować korzyści dla społeczeństwa i zminimalizować zagrożenia dla praw człowieka, demokracji i praworządności.

W konferencji wzięli udział eksperci wysokiego szczebla reprezentujący rządy, organizacje międzynarodowe, przedsiębiorstwa, technologie, środowisko akademickie, naukowe ośrodki badawcze, przedstawiciele społeczeństwa oraz media. Z punktu widzenia podstawowego mandatu

Rady Europy i jej wartości, debaty były poświęcone sposobom zapewnienia, by nowo powstające technologie były projektowane, opracowywane i stosowane w celu tworzenia wartości dla obywateli, społeczeństw demokratycznych oraz trwałości ram prawnych i instytucjonalnych.

2) 47. posiedzenie Biura Komitetu Konwencji 108. Paryż, 20-22.03.2019 r.

Program pierwszego w 2019 roku posiedzenia Biura był urozmaicony. Uczestnicy posiedzenia zapoznali się z kandydatami na stanowisko Sekretarza Generalnego i terminami dotyczącymi wyborów na to stanowisko. Ponadto pozyskali informacje w zakresie przyjęcia 13 lutego 2019 r. przez Komitet Ministrów deklaracji o potencjale manipulacyjnym procesów algorytmicznych oraz wynikach konferencji wysokiego szczebla „Zarządzanie przełomem – wpływ rozwoju sztucznej inteligencji na prawa człowieka, demokrację oraz rządy prawa", współorganizowanej przez fińską prezydencję Komitetu Ministrów.

Wydarzenie to odbyło się w dniach 26-27 lutego 2019 r. w Helsinkach. Zgromadzeni zapoznali się także ze stanem akcesji do Konwencji 108, w szczególności z dołączeniem do niej – jako 54 członka – Argentyny oraz z podpisaniem Konwencji 108+ przez Chorwację (22 marca 2019 r.), Włochy (5 marca 2019 r.), a także Cypr i Węgry (9 stycznia 2019 r.), co zwiększyło liczbę jej sygnatariuszy do 27.

Podczas spotkania pojawił się również temat aspektów technicznych i prawnych związanych z wykorzystaniem technologii rozpoznawania twarzy oraz kwestie ochrony danych w kontekście pomocy humanitarnej: technologii blockchain, tożsamości cyfrowej, sztucznej inteligencji i in. Uzgodniono, że kolejne posiedzenie plenarne ma zająć się wymogami ochrony danych w kontekście wdrażania Konwencji z Macolin w sprawie manipulacji rozgrywkami sportowymi.

Biuro przyjęło także zwycięzców Nagrody Stefano Rodoty, przyznanej w 2019 r. przez Komitet Konwencji 108. Nagroda przyznawana jest w uznaniu działalności Stefano Rodoty, wybitnego włoskiego prawnika i polityka, który poświęcił znaczną część swojego życia promowaniu dobrych praktyk w dziedzinie ochrony danych osobowych. Nagroda będzie przyznawana corocznie z okazji Dnia Ochrony Danych, jako wyraz uznania dla innowacyjnych i oryginalnych projektów badań naukowych w dziedzinie ochrony danych. W 2019 r. Nagroda Stefano Rodoty trafiła do do Ingridy Milkaite i Evy Lievens, autorek projektu, którego przedmiotem były badania prywatności i ochrony danych z perspektywy praw dziecka. Szczególną uwagę poświęcono także autorowi badań pod nazwą „Prawo do wymazania – ochrona informacji w samostanowieniu w społeczeństwie cyfrowym".

3) 29 Konferencja Europejskich Organów Ochrony Danych. Tbilisi, 8-10.05.2019 r.

Przedstawiciel Urzędu Ochrony Danych Osobowych uczestniczył w odbywającej się w Tbilisi 29. Konferencji Europejskich Organów Ochrony Danych, która zgromadziła przedstawicieli organów nadzorczych z Unii Europejskiej oraz krajów Partnerstwa Wschodniego.

W panelu pod nazwą „Przegląd Działań Podgrup Ochrony Danych" podsumowane zostały działania Grupy Państw Europy Środkowej i Wschodniej, której inicjatorem i koordynatorem jest polski organ nadzorczy. Wystąpienie przedstawiciela Urzędu wpisywało się również w obchodzoną w tym samym czasie dziesiątą rocznicę powstania Partnerstwa Wschodniego. Podczas wystąpienia w sesji poświęconej ochronie danych dzieci, zaprezentowane zostały działania Urzędu w zakresie ochrony danych osobowych dzieci oraz zapobiegania i przeciwdziałania cyberprzemocy. Uczestnicy panelu zgodni byli, że wciąż brakuje gotowych pomocy dydaktycznych dla nauczycieli i uczniów w zakresie ochrony danych najmłodszych obywateli. W tym kontekście duże zainteresowanie wzbudził projekt *„ARCADES”,* zainicjowany w 2014 r. przez polski organ nadzorczy, którego efektem była m.in. publikacja Europejskiego Podręcznika „Nauczanie o ochronie danych i prywatności w szkołach”[248].

W programie Konferencji znalazły się także tematy związane z: rocznym podsumowaniem wdrażania i egzekwowania przepisów RODO, nowatorskimi elementami zmodernizowanej Konwencji 108+, a także z wpływem organizacji międzynarodowych na podnoszenie standardów ochrony danych i prywatności.

Organizatorem tego wydarzenia było Biuro Inspektora Ochrony Danych Osobowych Gruzji.

4) 38 posiedzenie plenarne Komitetu T-PD. Strasburg, 13-14.06.2019 r.

Przedmiotem 38. Posiedzenia Komitetu T-PD była sytuacja polityczna i budżetowa Rady Europy związana z wyborami nowego Sekretarza Generalnego, decyzje podjęte podczas 129. Sesji Komitetu Ministrów (Helsinki, 16 - 17 maja 2019 r.), a także gotowość organizacji do wspierania wdrożenia Programu Pracy Komitetu na lata 2020-2021. Na posiedzeniu podjęto decyzję o utworzeniu grupy roboczej, której zadaniem jest opracowywanie metod i narzędzi ewaluacji oraz mechanizmu kontrolnego Konwencji 108+. W skład grupy roboczej wchodzić będzie Biuro Komitetu Konwencji oraz zainteresowane delegacje.

Uczestnicy posiedzenia podjęli decyzję o rozszerzeniu zakresu Programu Pracy Komitetu na lata 2020-2021 o:

[248] http://www.arcades-project.eu/images/pdf/arcades_teaching_handbook_final_PL.pdf

- włączenie współpracy z Grupą Kopenhaską i przyszłym Komitetem Konwencji Rady Europy w sprawie manipulacji rozgrywkami sportowymi (Konwencja z Macolin);
- włączenie ponownej analizy zalecenia *„CM/Rec(2010)13 Komitetu Ministrów dla państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili”*, podkreślając znaczenie wytycznych i innych instrumentów opracowanych przez Komitet, w szczególności dotyczących Big Data i sztucznej inteligencji;
- kwestie związane z technicznymi i prawnymi aspektami stosowania technologii rozpoznawania twarzy oraz ochroną danych i prywatności związanych z tą formą przetwarzania danych;
- włączenie współpracy z Komitetem Praw Dziecka (CAHENF) w zakresie ochrony danych dzieci w systemie edukacji.

5) IAPP Data Protection Intensive. Monachium, 18.09.2019 r.

Konferencja IAPP Data Protection Intensive zorganizowana była w Monachium przez International Association of Privacy Professionals. Przedstawiciel UODO wziął aktywny udział w panelu dyskusyjnym zatytułowanym „Punkt widzenia ustawodawcy”, podczas którego wraz z przedstawicielami innych organów ochrony danych z Unii Europejskiej dyskutowano o współpracy między organizacjami a organami nadzorczymi.

6) 48. Posiedzenie Biura Komitetu Konwencji 108. Paryż, 25-27.09.2019 r.

W 48. posiedzeniu Biura Komitetu Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych, przedstawiciel polskiego organu nadzorczego uczestniczył w charakterze obserwatora.

Podczas tego spotkania Sekretariat przestawił decyzję Komitetu Ministrów (CM/Del/Dec(2018)128/5), podkreślając znaczenie szybkiego przystąpienia do protokołu zmieniającego, wzywając państwa członkowskie do „natychmiastowego zainicjowania procesu prowadzącego do ratyfikacji, zatwierdzenia lub przyjęcia niniejszego protokołu zgodnie z ich prawem krajowym, nie później niż rok po dacie otwarcia protokołu do podpisu tj. 10 października 2018 r.”. Sekretariat przedstawił stan negocjacji w sprawie projektu drugiego protokołu dodatkowego do budapeszteńskiej konwencji o cyberprzestępczości (CETS nr 185). Powtórzył potrzebę zaangażowania Komitetu w opracowanie systemu ochrony danych drugiego protokołu dodatkowego, który powinien opierać się na Konwencji 108+, podkreślając konieczność uzyskania dodatkowych informacji na temat stanu negocjacji i koordynacji stanowisk krajowych.

Omówiono także temat współpracy z innymi organami Rady Europy, w szczególności z Komitetem Praw Dziecka (CAHENF) i Komitetem ekspertów ds. wymiarów praw człowieka w zakresie zautomatyzowanego przetwarzania danych i różnych form sztucznej inteligencji (MSI-AUT).

7) 41. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności – ICDPPC. Tirana, 21-24.10.2019 r.

Dyrektor Zespołu Współpracy Międzynarodowej i Edukacji reprezentowała Urząd podczas 41. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności. Tegoroczna Konferencja skupiła się na znalezieniu równowagi pomiędzy maksymalizacją potencjału współczesnego stylu życia obywateli oraz możliwościami technologicznymi, przy jednoczesnym zachowaniu wysokich standardów, ochrony danych i prywatności. W wyniku przeprowadzonych sesji powstała Rezolucja w sprawie Strategicznego Kierunku Konferencji na lata 2019-2021. Opiera się ona na trzech filarach: ewolucji w kierunku globalnych ram i standardów, ściślejszej współpracy w zakresie egzekwowania prawa oraz określaniu priorytetowych tematów polityki międzynarodowej.

41. ICDPPC uchwaliła:

- Rezolucję w sprawie promowania nowych, długoterminowych i praktycznych instrumentów oraz kontynuacji działań prawnych na rzecz skutecznej współpracy w zakresie transgranicznego egzekwowania prawa, która zachęca do dalszych starań na rzecz skuteczniejszej współpracy w postępowaniach transgranicznych i egzekwowaniu prawa.
- Rezolucję w sprawie uznania prywatności za podstawowe prawo człowieka i warunku wstępnego do wykonywania innych praw podstawowych, która bezpośrednio wzywa państwa członkowskie i grupy społeczne ze wszystkich sfer publicznych i prywatnych, w tym społeczeństwo obywatelskie i środowisko akademickie, do podjęcia konkretnych działań zapewniających ochronę podstawowych praw człowieka.
- Rezolucję wspierającą i ułatwiającą współpracę regulacyjną między organami ochrony danych a organami ochrony konsumentów i ochrony konkurencji w celu osiągnięcia jasnych i wysokich standardów ochrony danych w gospodarce cyfrowej, która przedłuża mandat Grupie Roboczej ds. Cyfrowych Obywateli i Konsumentów.
- Rezolucję dotyczącą czynnika ludzkiego, jako przyczyny naruszeń ochrony danych. Rezolucja wzywa wszystkich członków ICDPPC do promowania odpowiednich zabezpieczeń zapobiegającym błędom, które powstały wskutek czynnika ludzkiego i które mogą prowadzić do naruszenia danych osobowych, a także wzywa organizacje (w tym państwowe i prywatne),

aby zrozumiały, że naruszenia danych osobowych często wiążą się z błędami ludzkimi i w związku z tym powinny wdrożyć odpowiednie zabezpieczenia.

- Rezolucję w sprawie mediów społecznościowych i treści związanych z brutalnym ekstremizmem w Internecie. Rezolucja przedstawia konkretne działania, które miałyby zapobiec rozprzestrzenianiu się terroryzmu w mediach społecznościowych, a także zwalczać go za ich pośrednictwem.

8) Spotkanie partnerów projektu „T4DATA". Rzym, 14-15.11.2019 r.

W Rzymie podsumowano efekty działań edukacyjnych projektu „T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych" oraz podpisano porozumienie o dalszej współpracy. Zapewnia to dokument pod nazwą „Memorandum of Cooperation", podpisany przez konsorcjantów podczas tego spotkania, którego głównym wydarzeniem była Konferencja pt. „Podejście do wyzwania: spojrzenie na ochronę danych i nie tylko". Wydarzenie było nie tylko okazją do dyskusji na temat obecnego stanu prawnego, z jakim mamy do czynienia w związku ze stosowaniem ogólnego rozporządzenia o ochronie danych, ale również do dyskusji o wyzwaniach, jakie stoją przed inspektorami ochrony danych. Dwa lata realizacji projektu „T4DATA" przez UODO oraz organy nadzorcze z Włoch, Hiszpanii, Chorwacji i Bułgarii, umożliwiły powstanie materiałów i przedsięwzięć edukacyjnych dla inspektorów ochrony danych z sektora publicznego, takich jak „Podręcznik Inspektora Ochrony Danych"[249], czy platformy edukacyjne z wykładami dla inspektorów ochrony danych. Materiały te stanowią cenne wsparcie w procesie stosowania RODO.

Podczas rzymskiej konferencji partnerzy projektu „T4DATA" zaprezentowali krajowe doświadczenia z realizacji tego przedsięwzięcia. Uczestnicy projektu zorganizowali w swoich krajach łącznie 21 szkoleń, w których wzięło udział ponad cztery tysiące inspektorów. Powstało również pięć platform edukacyjnych przeznaczonych dla IOD z sektora publicznego, na których partnerzy projektu umieszczają wykłady dotyczące różnych aspektów stosowania RODO. Łącznie w krajach partnerskich odnotowano prawie siedem tysięcy logowań do platform edukacyjnych, które łącznie oferują już ponad 120 godzin wykładów. Jeśli chodzi o doświadczenia krajowe, to IOD z podmiotów publicznych mogą korzystać z platformy dostępnej pod adresem: https://t4data.uodo.gov.pl/. Ponadto Urząd Ochrony Danych Osobowych zorganizował dla IOD cztery lokalne szkolenia, których zapis jest również dostępny na wspomnianej platformie.

Pomimo że na początku stycznia 2020 roku nastąpiło formalne zakończenie projektu „T4DATA", to dzięki podpisanemu w Rzymie memorandum w dalszym ciągu uczestnicy projektu

[249] https://uodo.gov.pl/pl/168/1298

będą upowszechniać rezultaty tej inicjatywy. Materiały edukacyjne dla IOD, takie jak platforma z wykładami oraz zapis z lokalnych szkoleń, będą udostępniane kolejnym grupom inspektorów działających w administracji publicznej.

9) 39. Posiedzenie plenarne Komitetu T-PD. Strasburg, 19-21.11.2019 r.

Listopadowe posiedzenie Komitetu T-PD skupiło się wokół aktualizacji Rekomendacji dotyczącej profilowania (CM/Rec(2010)13,) kwestii związanych z rozpoznawaniem twarzy oraz ochrony danych w systemach edukacyjnych. Dużo uwagi poświęcono opracowywanej przez Komitet T-PD procedurze kontroli przestrzegania wymogów Konwencji 108+. Komitet przyjął opinię T-PD(2019)8rev dotyczącą bezpośredniego ujawnienia informacji o subskrybentach w związku z projektem drugiego protokołu dodatkowego do konwencji budapesztańskiej, a także opinię T-PD(2019)09 dotyczącą Zalecenia Komitetu Ministrów dla państw członkowskich w sprawie wpływu systemów algorytmicznych na prawa człowieka. Biuro Komitetu T-PD zostało zobowiązane do zinterpretowania terminu „operacje arytmetyczne" użytego w art. 2 Konwencji 108+, a także do dokonania rozróżnienia pomiędzy statusem prawnym „administratora danych" a „odbiorcą" oraz wypracowania wytycznych dotyczących anonimizacji i pseudonimizacji w odniesieniu do „osoby zidentyfikowanej lub możliwej do zidentyfikowania".

39. posiedzenie plenarne T-PD odbyło się przy okazji Konferencji Octopus 2019. Delegaci mieli okazję uczestniczyć w drugim warsztacie konferencji pt. „Ochrona danych i wymiar sprawiedliwości w sprawach karnych", podczas której dyskutowano nad zapewnieniem spójności między Konwencją 108+ a drugim protokołem dodatkowym do konwencji budapesztańskiej.

10) Konferencja „Dane to wartość – chroń ją". Ryga, 26.11.2019 r.

Organizatorem konferencji „Dane to wartość – chroń ją!", był łotewski organ ochrony danych osobowych. Konferencja miała na celu podsumowanie dotychczasowych działań w zakresie edukacji sektora MŚP, w ramach pierwszej części projektu współfinansowanego ze środków Komisji Europejskiej, pod nazwą „General Data Protection Regulation – possibilities and responsibilities for small and medium-sized enterprises; rights and risks for minors (DPSME)".

W ramach projektu zostało zorganizowanych 10 seminariów, podczas których uczestnicy – przedstawiciele sektora mikro, małych i średnich przedsiębiorstw (MŚP) – mogli podnieść swoją świadomość w zakresie stosowania RODO. W sumie w konferencji wzięło udział ponad 400 uczestników. Głównymi tematami konferencji były podstawy ogólnego rozporządzenia o ochronie danych, odpowiedzialność regulacyjna administratora, sposoby zapewnienia wdrożenia wymagań technicznych i organizacyjnych w firmie, rola Europejskiej Rady Ochrony Danych w kontekście rozporządzenia oraz mechanizm kompleksowej obsługi. Prelegentami konferencji byli zarówno

mówcy lokalni, jak i zagraniczni, w tym: przedstawiciel UODO oraz Wiceprzewodniczący Europejskiej Rady Ochrony Danych.

11) 33. Międzynarodowa Konferencja Czerwonego Krzyża i Czerwonego Półksiężyca. Genewa, 9-12.12.2019 r.

Przedstawiciel UODO, jako członek Komisji ds. Międzynarodowego Prawa Humanitarnego przy Ministerstwie Spraw Zagranicznych, był członkiem delegacji polskiej na 33. Międzynarodową Konferencję Czerwonego Krzyża i Czerwonego Półksiężyca (MK), która odbyła się w dniach 9-12 grudnia 2019 r. w Genewie, z udziałem ponad 190 delegacji krajowych. Konferencja stanowiła unikalne forum dyskusji nt. zapewnienia ochrony osobom dotkniętym konfliktami zbrojnymi, klęskami żywiołowymi i innymi sytuacjami nadzwyczajnymi, w związku z aktualnymi wyzwaniami związanymi z nowymi technologiami, nowymi rodzajami broni i nowymi sytuacjami, w których występują konflikty (miasta, cyberprzestrzeń) oraz zapewnienia właściwych warunków świadczenia pomocy humanitarnej.

Podczas tego wydarzenia uchwalona została rezolucja „Przywracanie Więzów Rodzinnych przy jednoczesnym poszanowaniu prawa do prywatności, w tym także w zakresie ochrony danych osobowych". Rezolucja uznaje, że sprawą najwyższej wagi jest zapewnienie, aby przetwarzanie i przekazywanie danych osobowych między komponentami Międzynarodowego Ruchu IRCR, szczególnie w ramach Przywracania Więzów Rodzinnych, pozostało nieograniczone pod warunkiem przestrzegania Kodeksu Postępowania w zakresie ochrony danych, Międzynarodowego Prawa Humanitarnego i Statutu Ruchu.

Międzynarodowa Konferencja uznała także, że niewłaściwe wykorzystanie danych osobowych może prowadzić do naruszenia obowiązków w zakresie ochrony prywatności określonych w krajowych, regionalnych i międzynarodowych ramach prawnych i może mieć poważny wpływ na bezpieczeństwo osób objętych działaniami Międzynarodowego Ruchu. Dokument zwraca też uwagę na trudności, czasem wręcz brak możliwości, uzyskania zgody na przetwarzanie danych osób zaginionych lub członków rozdzielonych rodzin i konsekwentnym poleganiu na alternatywnych podstawach przetwarzania danych osobowych, tj. interesie publicznym, żywotnym interesie i przestrzeganiu zobowiązania prawnego. Ilekroć jakikolwiek komponent Międzynarodowego Ruchu zbiera lub w inny sposób przetwarza dane osobowe w ramach Przywracania Więzów Rodzinnych, powinien to robić wyłącznie w celach o charakterze humanitarnym.

V. Podsumowanie

Przechodząc do podsumowania niniejszego *Sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019* podkreślić należy, że wyraźny wzrost liczby wpływających do Urzędu skarg osób, których dane dotyczą, z jednej strony wskazuje na problemy z przestrzeganiem przez administratorów prawa tych osób do ochrony danych, z drugiej jednak strony wskazywać może także na wzrost świadomości tych osób, co do przysługujących im praw. Odnotować należy także znaczny wzrost liczby wpływających do UODO pytań prawnych dotyczących stosowania RODO, jak i zgłoszeń naruszeń ochrony danych, dokonywanych przez administratorów. Powyższe pozwala stwierdzić, że choć poziom znajomości obowiązujących przepisów o ochronie danych osobowych stale wzrasta, to obecnie konieczne jest dalsze prowadzenie działań edukacyjnych skierowanych do podmiotów danych, jak i administratorów. Tym samym należy podkreślić że poza podstawowymi działaniami Urzędu, jakimi są m.in. rozpatrywanie skarg obywateli dotyczących naruszeń w zakresie przetwarzania ich danych osobowych, czy prowadzenie działalności legislacyjnej, konieczne jest kontynuowanie zapoczątkowanych w latach poprzednich, działań upowszechniających wiedzę o ochronie danych osobowych i przepisach regulujących tę materię. Działania informacyjno-edukacyjne prowadzą do zwiększania świadomości i ugruntowania się wiedzy administratorów, podmiotów przetwarzających dane osobowe na zlecenie administratorów, jak i podmiotów danych, co przyczyni się do wzrostu bezpieczeństwa procesów przetwarzania danych osobowych w Polsce.

Dziś już możemy stwierdzić, że po upływie pierwszego roku stosowania nowego prawa o ochronie danych osobowych udało się UODO zmienić postrzeganie przepisów rozporządzenia, jako nieracjonalnych i groźnych dla przedsiębiorców. Nikt nie ma złudzeń, że trudno jest rozwijać gospodarkę bez przetwarzania danych osobowych i dlatego można już dostrzec próby szukania równowagi pomiędzy prawem do prywatności a swobodą przetwarzania danych. Coraz większa świadomość obywateli sprawiła, że biznes zaczął uwzględniać ich prawo do prywatności i ochrony danych osobowych. Na pozytywną ocenę zasługuje też wzrost świadomości wśród społeczeństwa, ale trzeba kontynuować pracę nad zapewnieniem, żeby przepisy RODO działały sprawnie. Zapewnienie właściwego stosowania RODO w praktyce będzie wciąż jeszcze wymagać czasu i wielu działań informacyjno-edukacyjnych organu.

Rok 2020 będzie rokiem pierwszego całościowego przeglądu działania przepisów RODO. Zadanie to wynika wprost z art. 97 ogólnego rozporządzenia o ochronie danych osobowych. Na mocy tego przepisu Komisja Europejska po raz pierwszy przedstawiła Parlamentowi

Europejskiemu oraz Radzie sprawozdanie z oceny i przeglądu RODO[250]. W chwili obecnej prowadzona jest w Unii Europejskiej dyskusja na temat sektorowych przepisów dotyczących ochrony danych.

[250] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020DC0264&from=EN. Zob. także komunikat prasowy KE z 24.06.2020 r. https://ec.europa.eu/commission/presscorner/detail/pl/ip_20_1163 .

ZAŁĄCZNIKI

Załącznik nr 1

Wykaz szkoleń przeprowadzonych przez UODO w 2019 r.

L.p.	Data szkolenia	Miejscowość	Podmiot szkolony
1.	14.01.2019	Warszawa	Szkolenie dla IOD pt. „Zgłaszanie naruszenia ochrony danych". Organizator: UODO.
2.	16.01.2019	Warszawa	Szkolenie dla kadry zarządzającej MSWiA.
3.	16.01.2019	Warszawa	Szkolenie dla IOD Komendy Głównej Policji.
4.	7.02.2019	Łódź	Szkolenie przedstawicieli jednostek samorządu terytorialnego. Organizatorzy: UODO oraz NIST.
5.	8.02.2019	Toruń	Szkolenie przedstawicieli jednostek samorządu terytorialnego. Organizatorzy: UODO oraz NIST.
6.	12.02.2019	Warszawa	Szkolenie dla IOD pt. „Zasady przetwarzania danych osobowych w świetle ustawy wdrażającej dyrektywę 2016/680". Organizator: UODO.
7.	20.02.2019	Warszawa	Szkolenie IOD pt. „Przekazywanie danych do państw trzecich". Organizator: UODO.
8.	28.02.2019	Warszawa	Szkolenie IOD pt. „Obowiązek informacyjny". Organizator: UODO.
9.	6.03.2019	Olsztyn	Szkolenie przedstawicieli jednostek samorządu terytorialnego. Organizatorzy: UODO oraz NIST.
10.	28.03.2019	Warszawa	Szkolenie pt. „Ochrona danych osobowych w instytucjach publicznych w świetle obowiązujących przepisów UE (RODO) dla pracowników pionów merytorycznych Centrali KRUS.
11.	11.04.2019	Warszawa	Odprawa szkoleniowa dla IOD w MSWiA.
12.	17.04.2019	Warszawa	Szkolenie dla przedstawicieli Regionalnej Dyrekcji Ochrony Środowiska z siedzibą w Łodzi.
13.	9.05.2019	Warszawa	Szkolenie dla sędziów Krajowej Rady Sądownictwa.
14.	27.05.2019	Poznań	Szkolenie przedstawicieli organów publicznych i urzędników służby cywilnej w ramach projektu „T4DATA".
15.	29.05.2019	Warszawa	Szkolenie pt. „Ochrona danych osobowych w instytucjach publicznych w świetle obowiązujących przepisów UE (RODO)" dla pracowników pionów merytorycznych Centrali KRUS.
16.	31.05.2019	Gdynia	Szkolenie przedstawicieli organów publicznych i urzędników służby cywilnej w ramach projektu „T4DATA".
17.	10.06.2019	Rzeszów	Szkolenie przedstawicieli organów publicznych i urzędników służby cywilnej w ramach projektu „T4DATA".
18.	18.06.2019	Warszawa	Szkolenie przedstawicieli organów publicznych i urzędników służby cywilnej w ramach projektu „T4DATA".

19.	5.09.2019	Warszawa	Szkolenie dla wojewodów, kadry zarządzającej oraz IOD działających w Urzędach Wojewódzkich. Organizator: MSWiA.
20.	27.09.2019	Warszawa	VI dzień otwarty dla służby cywilnej – Kancelaria Premiera Rady Ministrów.
21.	2-3.10.2019	Warszawa	Konferencja szkoleniowa dla uczestników X edycji Programu TDTS. Organizatorzy: UODO.
22.	8.10.2019	Warszawa	Warsztat szkoleniowy dla IOD z kuratorów oświaty. Organizatorzy: UODO, MEN.
23.	14.10.2019	Warszawa	Szkolenie dla pracowników Biura Komisji Sejmowych i Ośrodka Informatyki. Kancelaria Sejmu.
24.	25.10.2019	Warszawa	I Forum Wolontariatu – konsultacje prawne. Organizator: NIW.
25.	20.11.2019	Warszawa	Szkolenie kadry zarządzającej i IOD samodzielnych publicznych ZOZ MSWiA. Organizator: Departament Zdrowia MSWiA.

Załącznik nr 2

Wykaz wydarzeń objętych patronatem Prezesa UODO w 2019 r.

1. Dzień IOD. Konferencja „Pierwsze doświadczenia pełnienia funkcji Inspektora Ochrony Danych". Organizator: SABI – Stowarzyszenie Inspektorów Ochrony Danych, Wydział Zarządzania Politechniki Warszawskiej. Warszawa, 24 stycznia 2019 r.
2. V Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej. Organizator: Akademia Wyższej Szkoły Biznesu w Dąbrowie Górniczej. Dąbrowa Górnicza, 1 lutego 2019 r.
3. Konferencja „Młode Forum Prawa Mediów Elektronicznych". Organizator: Studenckie Centrum Kultury Uniwersytetu Opolskiego. Opole, 8 kwietnia 2019 r.
4. VII edycja Ogólnopolskiego Szczytu Energetycznego OSE. Organizator: Europejskie Centrum Biznesu. Gdańsk, 8-9 kwietnia 2019 r.
5. VI Forum Kierowników IT w Administracji. Organizator: redakcja miesięcznika „IT w Administracji". Zakopane, 10-12 kwietnia 2019 r.
6. Konferencja „Ochrona danych medycznych w dobie nowych technologii". Organizator: Koło Naukowe Prawa Medycznego Uniwersytetu Jagiellońskiego. Kraków, 12 kwietnia 2019 r.
7. 3. edycja Konferencji RIBA Forum 2019. Organizator: Evention Sp. z o. o. Falenty k/Warszawy, 16-17 kwietnia 2019 r.
8. Ogólnopolska Konferencja Naukowa „Prawo w dobie cyfryzacji". Organizator: Wydział Prawa i Administracji Uniwersytet Mikołaja Kopernika w Toruniu. Toruń, 17 kwietnia 2019 r.
9. XI Konferencja Naukowa „Bezpieczeństwo w Internecie – Analityka danych". Organizatorzy: UKSW w Warszawie, Urząd Ochrony Danych Osobowych, Naukowe Centrum Prawno-Informatyczne. Warszawa, 6-7 czerwca 2019 r.
10. VIII Konwent Ochrony Danych Osobowych i Informacji pt. "D(RODO)wskazy, czyli nowe kierunki ochrony danych w biznesie". Organizatorzy: Lubasz i Wspólnicy – Kancelaria Radców Prawnych oraz FORSAFE sp. z o.o. Łódź, 21 listopada 2019 r.
11. Ogólnopolska kampania edukacyjna dotycząca bezpieczeństwa w sieci, która odbywa się w ramach obchodów Międzynarodowego Dnia Ochrony Danych Osobowych. Organizator: Śląska Sieć Metropolitarna w Gliwicach.
12. Ogólnopolska kampania edukacyjna „RODO dla pacjenta". Organizator: Kancelaria Domański Zakrzewski Palinka.

Załącznik nr 3

Wykaz konferencji, seminariów, spotkań krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2019 r. w Polsce przez UODO lub inne podmioty.

L. p.	Data	Konferencja/Seminarium	Miejsce
1.	24.01.2019	Ogólnopolska Konferencja pt. „Pierwsze doświadczenia wykonywania funkcji Inspektora Ochrony Danych" w ramach obchodów Dnia Inspektora Ochrony Danych. Organizator: Stowarzyszenie Inspektorów Ochrony Danych – SABI.	Warszawa
2.	28.01.2019	XIII Dzień Ochrony Danych Osobowych. Konferencja „System ochrony danych osobowych po wprowadzeniu reformy". Organizator: UODO.	Warszawa
3.	1.02.2019	V Dzień Otwarty UODO w Akademii Wyższej Szkoły Biznesu w Dąbrowie Górniczej, z okazji XIII Dnia Ochrony Danych Osobowych 2019. Organizator: Akademia WSB w Dąbrowie Górniczej.	Dąbrowa Górnicza
4.	22.02.2019	Posiedzenie Konferencji Rektorów Polskich Uczelni Technicznych – KRPUT. Organizator: Politechnika Częstochowska.	Częstochowa
5.	27.02.2019	Konferencja „RODO w sektorze medycznym – gdzie jesteśmy, dokąd zmierzamy? – edycja II". Organizatorzy: Polska Federacja Szpitali, Uczelnia Łazarskiego oraz Domański Zakrzewski Palinka sp.k.	Warszawa
6.	1.03.2019	Spotkanie edukacyjne „360° Master Panel". Organizator: Towarzystwo Chirurgów Polskich oraz Johnson & Johnson Sp. z o.o.	Warszawa
7.	18-19.03.2019	III Forum ABI EXPERT. Organizator: Redakcja kwartalnika „ABI Expert".	Łochów k/Warszawy
8.	25.03.2019	Seminarium Naukowe dla studentów wydziałów prawa i administracji z Torunia, Białegostoku i Gdańska. Organizator: UODO.	Warszawa
9.	29.03.2019	Konferencja w ramach Ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", pt. „#RODO w edukacji. Mazowieckie spotkanie z ochroną danych osobowych w szkole". Organizator: UODO, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.	Siedlce
10.	30.03.2019	Wykład inauguracyjny „Pierwsze doświadczenia organu nadzorczego w zakresie wdrażania przepisów o ochronie danych osobowych", podczas uroczystości otwarcia XVII edycji Podyplomowego Studium Ochrony Danych Osobowych w Akademii Leona Koźmińskiego w roku akademickim 2018/2019.	Warszawa
11.	3.04.2019	„#RODO w edukacji. Łódzkie spotkanie z ochroną danych osobowych w szkole". Trzecie z cyklu spotkanie w ramach ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa". Organizator: UODO, Zespół Szkół i Placówek Oświatowych Województwa Łódzkiego w Sieradzu.	Sieradz
12.	3.04.2019	Konferencja „Compliance Day 2019". Organizator: Instytut Compliance.	Warszawa
13.	8.04.2019	Konferencja Młode Forum Mediów Elektronicznych. Organizator: Studenckie Centrum Kultury Uniwersytetu Opolskiego.	Opole

14.	8.04.2019	VII Ogólnopolski Szczyt Energetyczny OSE Gdańsk 2019. Organizator: Europejskie Centrum Biznesu.	Gdańsk
15.	11.04.2019	VI Forum Kierowników IT w Administracji. Organizator: Redakcja miesięcznika „IT w Administracji".	Zakopane
16.	11.04.2019	Odprawa szkoleniowa Inspektora Nadzoru Wewnętrznego MSWiA dla IOD powołanych na poziomie jednostek centralnych oraz wojewódzkich w służbach nadzorowanych przez Ministra właściwego do spraw wewnętrznych.	Warszawa
17.	12.04.2019	Konferencja „Ochrona danych medycznych w dobie nowych technologii". Organizator: Koło Naukowe Prawa Medycznego UJ.	Kraków
18.	16-17.04.2019	RIBA Forum 2019. Organizator: Evention sp. z o.o.	Falenty k/Warszawy
19.	15.04.2019	Konferencja „RODO rok po wdrożeniu". Organizator: Firma Bonnier Business Polska wydawca dziennika Puls Biznesu.	Warszawa
20.	15.04.2019	Ogólnopolska Konferencja Naukowa „Prawo Mediów Społecznościowych". Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Olsztyn.	Olsztyn
21.	15.04.2019	XI Międzynarodowa Konferencja Naukowa „Ochrona praw człowieka w dobie kryzysu demokracji liberalnej". Organizatorzy: Wydział Prawa, Administracji i Zarządzania Uniwersytetu Jana Kochanowskiego w Kielcach oraz Zarząd Główny Stowarzyszenia Parlamentarzystów Polskich.	Warszawa
22.	17.04.2019	Spotkanie Liderów Bankowości i Ubezpieczeń 2019. Organizator: MM Conferences S.A.	Warszawa
23.	18.04.2019	Spotkanie audytorów wewnętrznych z jednostek sektora finansów publicznych nt. świadczenia usług zapewniających w obszarze ochrony danych osobowych". Organizator: Ministerstwo Finansów.	Warszawa
24.	29.04.2019	Debata finałowa cyklu debat na temat cyberbezpieczeństwa oraz ochrony danych osobowych pt. „Moje dane są bezpieczne w naszej szkole w dobie Internetu Wszechrzeczy (IoE)". Organizator: Młodzieżowa Rada Miasta Jaworzna.	Jaworzno
25.	8.05.2019	Warsztat na temat dezinformacji – wybory europarlamentarne 2019. Organizator: NASK.	Warszawa
26.	9.05.2019	Ogólnopolska Konferencja Naukowa pt. „RODO – od analizy modelu do stosowania prawa". Organizatorzy: WPiA UJ, Okręgowa Izba Radców Prawnych w Krakowie.	Kraków
27.	14.05.2019	Europejski Kongres Gospodarczy 2019. Organizator: Polskie Towarzystwo Wspierania Przedsiębiorczości S.A.	Katowice
28.	16.05.2019	Konferencja „Przetwarzanie danych osobowych przez mikro, małe i średnie przedsiębiorstwa w świetle przepisów RODO". Organizator: Akademia WSB w Dąbrowie Górniczej.	Dąbrowa Górnicza
29.	16.05.2019	Konferencja Naukowa pt. „Rok RODO". Organizatorzy: Katedra Prawa Gospodarczego Publicznego Uniwersytetu Gdańskiego (UG), Katedra Ochrony Środowiska UG oraz Zakład Informatyki Prawniczej UG.	Gdańsk
30.	22.05.2019	VI Ogólnopolska Konferencja Samorządu i Oświaty „Edukacja przyszłości". Organizator: redakcja pisma samorządu terytorialnego „WSPÓLNOTA".	Lublin
31.	22.05.2019	Impact'19. Panel dyskusyjny pt. „Dlaczego potrzebujemy strategii AI w zdrowiu?" Organizator: Fundacja Impact, Kancelaria Domański Zakrzewski Palinka Sp.k.	Kraków
32.	22.05.2019	Seminarium Unii Metropolii Polskich pt. „RODO – rok obowiązywania nowych regulacji prawnych związanych z ochroną danych osobowych".	Lublin
33.	30.05.2019	Spotkanie pt. „Rodo już rok z nami. Projekt e-OpenSpace". Organizatorzy: UODO, Uniwersytet Jagielloński.	Warszawa

34.	4.06.2019	XXII Szkoła Zarządzania Strategicznego Fundacji Rektorów Polskich dla kanclerzy i kwestorów (dyrektorów finansowych). Organizatorzy: Fundacja Rektorów Polskich oraz Konferencja Rektorów Akademickich Szkół Polskich.	Warchały k/Szczytna
35.	5.06.2019	VI Kongres Zarządzania Administracją Samorządową. Organizatorzy: Municipium oraz redakcja pisma samorządu terytorialnego „WSPÓLNOTA".	Wrocław
36.	6.06.2019	VII Kongres Prawa Bankowego i Informacji. Organizator: Związek Banków Polskich.	Warszawa
37.	05.06.2019	Konferencja CDO Forum 2019, pt. „Dane nieosobowe i kontekst regulacji europejskich dotyczących danych".	Warszawa
38.	6.06.2019	Międzynarodowa Konferencja pt. „Dawniej niż wczoraj – 100 lat Polskiej Policji". Organizatorzy: Wydział Policyjnych Nauk Stosowanych Wyższej Szkoły Policji w Szczytnie, Instytut Pamięci Narodowej Oddział w Białymstoku, Delegatura Instytutu Pamięci Narodowej w Olsztynie.	Szczytno
39.	6-7.06.2019	XI Konferencja z cyklu „Bezpieczeństwo w Internecie" dot. analityki danych. Organizator: UKSW, UODO, Koło Naukowe Centrum Prawno-Informatyczne.	Warszawa
40.	7.06.2019	Konferencja XIX Majowe Mrozy. Organizatorzy: Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie, Polsko-Japońska Akademia Technik Komputerowych oraz Miasto i Gmina Mrozy.	Warszawa
41.	10.06.2019	Konferencja „Podsumowanie pierwszego roku obowiązywania RODO w jednostkach samorządu terytorialnego". Organizatorzy: UODO, Sejmowa Komisja Samorządu Terytorialnego i polityki Regionalnej oraz Narodowy Instytut Samorządu Terytorialnego – NIST.	Warszawa
42.	11.06.2019	Seminarium podsumowujące IX edycję programu „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Organizator: Urząd Ochrony Danych Osobowych.	Warszawa
43.	11.06.2019	Konferencja pt. „Przygotuj się do kontroli UODO". Organizator: „Wiedza i Praktyka".	Warszawa
44.	13.06.2019	Seminarium Naukowe dt. tworzenia kodeksów postępowania w oświacie. Organizatorzy: Urząd Miasta Częstochowy, Fundacja Niech Się Dzieje oraz Zespół Szkół Samochodowo-Budowlanych w Częstochowie.	Częstochowa
45.	14.06.2019	Konferencja „Praktyczne problemy ogólnego rozporządzenia o ochronie danych – refleksje po roku doświadczeń". Organizator: Katedra polityki Gospodarczej WPiA Uniwersytetu Jagiellońskiego.	Kraków
46.	27.06.2019	Konferencja „RODO w instytucjach finansowych – pierwsze doświadczenia, interpretacje oraz nowe przepisy. Organizator: Puls Biznesu. Partner merytoryczny: Kancelaria Traple Konarski Podrecki i Wspólnicy.	Warszawa
47.	1-5.07.2019	Work shadowing project – wizyta prof. dr Dieter-a Kugelmann-a z DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz w Urzędzie Ochrony Danych Osobowych.	Warszawa
48.	29.07.2019	Konferencja z okazji 100. rocznicy powstania Policji Państwowej. Organizator: Wyższa Szkoła Policji w Szczytnie.	Szczytno
49.	20.08.2019	IV Spotkanie partnerów projektu „e-OpenSpace". Podsumowanie projektu. Organizator: UODO.	Warszawa
50.	3-5.09.2019	XXIX Forum Ekonomiczne „Europa jutra. Silna, czyli jaka?". Organizator: Fundacja Instytut Studiów Wschodnich.	Krynica Zdrój
51.	5.09.2019	Wideokonferencja „Ochrona danych osobowych w świetle RODO" dla wojewodów i kadry zarządzającej oraz IOD urzędów wojewódzkich. Organizator: MSWiA.	Warszawa

52.	24.09.2019 r.	Spotkanie dt. prezentacji raportu „Zjawisko dezinformacji w dobie cyfrowej rewolucji. Państwo. Społeczeństwo. Polityka. Biznes". Organizator: NASK.	Warszawa
53.	27.09.2019	VII Dzień otwarty dla służby cywilnej w Kancelarii Premiera Rady Ministrów. Organizator: Departament Służby Cywilnej KPRM.	Warszawa
54.	30.09.2019	Inauguracja roku akademickiego 2019/2020 w SGGW.	Warszawa
55.	1.10.2019	„Strategic Cyber Forum – CyberDefence24 Day".	Warszawa
56.	1.10.2019	Konferencja inaugurująca rozpoczęcie X edycji ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Organizatorzy: Urząd Ochrony Danych Osobowych oraz Zespół ds. Bezpieczeństwa Dzieci i Młodzieży w Świecie Wirtualnym, Senat RP.	Rojów
57.	2.10.2019	XVII Samorządowe Forum Kapitału i Finansów. Konferencja tematyczna „Forum Przewodniczących Rad". Organizatorzy: Redakcja Pisma Samorządu Terytorialnego „WSPÓLNOTA" oraz Międzykomunalna Spółka Akcyjna Municipium.	Katowice
58.	2-3.10.2019	Konferencja szkoleniowo-informacyjna X edycji programu TDTS. Organizatorzy: Urząd Ochrony Danych Osobowych oraz Zespół ds. Bezpieczeństwa Dzieci i Młodzieży w Świecie Wirtualnym, Senat RP.	Warszawa
59.	3.10.2019	Inauguracja roku akademickiego 2019/2020 w Akademii Leona Koźmińskiego w Warszawie.	Warszawa
60.	3-4.10.2019	Konferencja Translating Europe Workshop poświęcona dobrym praktykom korzystania z tłumaczenia maszynowego. Organizator: Departament Języka Polskiego DGT Komisji Europejskiej.	Warszawa
61.	4.10.2019	Inauguracja roku akademickiego 2019/2020 w Wyższej Szkole Policji w Szczytnie.	Szczytno
62.	7-8.10.2019	IV Kongres 590.	Jasionka k/Rzeszowa
63.	8.10.2019	Warsztat dla Inspektorów Ochrony Danych z kuratoriów oświaty. Organizatorzy: UODO oraz MEN.	Warszawa
64.	8.10.2019	Inauguracja jubileuszowego 25. Roku Akademickiego w Akademii Wyższej Szkoły Biznesu w Dąbrowie Górniczej.	Dąbrowa Górnicza
65.	14.10.2019	Obchody 20-lecia UKSW w Warszawie oraz inauguracja roku akademickiego 2019/2020 na UKSW w Warszawie.	Warszawa
66.	14.10.2019	Szkolenie z zakresu ochrony danych osobowych dla pracowników Biura Komisji Sejmowych i Ośrodka Informatyki Kancelarii Sejmu. Organizator: Biuro Prawne i Spraw Pracowniczych Kancelarii Sejmu RP.	Warszawa
67.	15.10.2019	Wykład Profesora Johna M. Czarnetzky'ego pt. „Prawo gospodarcze w świetle katolickiej nauki społecznej". Organizator: Prezes Trybunału Konstytucyjnego.	Warszawa
68.	16-17.10.2019	Wizyta studyjna przedstawicieli białoruskich organów publicznych w Urzędzie Ochrony Danych Osobowych. Organizator: UODO w ramach programu Rady Europy pt. „Poprawa ochrony danych w Republice Białorusi".	Warszawa
69.	19.10.2019	Inauguracja 18. edycji Podyplomowego Studium Ochrony Danych Osobowych w Akademii Leona Koźmińskiego w Warszawie.	Warszawa
70.	21.10.2019	Konferencja „Rewolucja cyfrowa zagrożeniem dla pracowników sektora usług". Organizator: Rada krajowego Sekretariatu Banków, Handlu i Ubezpieczeń NSZZ „Solidarność".	Warszawa
71.	22.10.2019	Spotkanie dt. prezentacji Raportu pt.: „RODO. Rok obowiązywania. Interpretacje i dobre praktyki branży reklamy internetowej" Organizator: Związek Pracodawców Branży Internetowej IAB Polska.	Warszawa

72.	24-25.10.2019	I Forum Wolontariatu inaugurujące rządowy Program Korpusu Solidarności. Organizator: Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego.	Warszawa
73.	25.10.2019	Konferencja inaugurująca V edycję Studiów podyplomowych „Wykonywanie funkcji inspektora ochrony danych" w Instytucie Nauk Prawnych PAN.	Warszawa
74.	29-30.10.2019	V Forum Cyberbezpieczeństwa – CYBERSEC. Organizator: Instytut Kościuszki.	Katowice
75.	19.11.2019	VIII Konwent Ochrony Danych i Informacji pt. „D(RODO)wskazy, czyli nowe kierunki ochrony danych w biznesie". Organizatorzy: Lubasz i Wspólnicy Kancelaria Radców Prawnych oraz FORSAFE sp. z o.o.	Łódź
76.	19.11.2019	XIII Seminarium Warszawskie pt. „Prawa dziecka w świetle Europejskiej Konwencji Praw Człowieka". Organizatorzy: Ministerstwo Spraw Zagranicznych oraz Rzecznik Praw Dziecka.	Warszawa
77.	20.11.2019	Konferencja szkoleniowa dla kadry zarządzającej samodzielnymi publicznymi ZOZ MSWiA oraz IOD placówek ochrony zdrowia. Organizator: Departament Zdrowia MSWiA.	Warszawa
78.	21.11.2019	Konferencja podsumowująca realizację projektu pn. Platforma Usług Elektronicznych Urzędu Patentowego. Organizator: Polska Izba Informatyki i Telekomunikacji.	Rawa Mazowiecka
79.	26.11.2019	Uroczystość wręczenia nagród Głównego Inspektora Pracy.	Warszawa
80.	26.11.2019	Konferencja „Analiza i bezpieczeństwo zasobów informacyjnych – problemy prawne, naukowe i techniczne". Organizatorzy: ZUS, GUS i WAT.	Warszawa
81.	27.11.2019	Posiedzenie Komisji ds. Międzynarodowego Prawa Humanitarnego w siedzibie Ministerstwa Spraw Zagranicznych. Organizator: Departament Prawno-Traktatowy MSZ.	Warszawa
82.	3-4.12.2019	24. Kongres Inspektorów Ochrony Danych: Wiedza - Praktyka - Zgodność, pt. Audyt wdrożenia RODO – 2019". Organizator: Kancelaria Ekspertów ENSI.	Siła k/Olsztyna
83.	9.12.2019	Inauguracja 3. ed. Studium dla inspektorów ochrony danych w sektorze publicznym. Organizatorzy: UODO oraz KSAP.	Warszawa
84.	9.12.2019	Uroczystości związane z obchodami 20-lecia UKSW w Warszawie.	Warszawa
85.	10.12.2019	Posiedzenie Zespołu ds. Europejskiego Trybunału Praw Człowieka. Organizator: Departament Prawno -Traktatowy MSZ.	Warszawa
86.	13.12.2019	VII Krajowe Forum Ochrony Infrastruktury Krytycznej. Organizator: Rządowe Centrum Bezpieczeństwa.	Warszawa

Załącznik nr 4

Wykaz konferencji, seminariów, spotkań i innych wydarzeń międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, które odbyły się w 2019 r. za granicą.

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	14-17.01.2019	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup) oraz Podgrupy ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
2.	15-16.01.2019	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
3.	17.01.2019	III Spotkanie partnerów projektu „e-OpenSpace".	Mediolan
4.	22-23.01.2019	6.posiedzenie plenarne Europejskiej Rady Ochrony Danych.	Bruksela
5.	29.01.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
6.	30.01.2019	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup - SAS).	Bruksela
7.	30-31.01.2019	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health - CEH) Europejskiej Rady Ochrony Danych.	Bruksela
8.	1.02.2019	Warsztaty EIOD dotyczące wyborów (EDPS Election Workshop).	Bruksela
9.	11-12.02.2019	7. posiedzenie plenarne Europejskiej Rady Ochrony Danych (EROD) oraz spotkanie EIOD dotyczące wyborów i ochrony danych.	Bruksela
10.	11-12.02.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
11.	19-20.02.2019	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
12.	20-21.02.2019	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
13.	20-21.02.2019	Posiedzenie Podgrupy ds. Nakładania Kar (Fining Task Force) Europejskiej Rady Ochrony Danych.	Bruksela
14.	21-22.02.2019	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement)	Bruksela
15.	25.02.2019	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH) Europejskiej Rady Ochrony Danych.	Bruksela
16.	25-26.02.2019	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
17.	25-27.02.2019	High-Level Conference nt. wpływu rozwoju AI na prawa człowieka, demokrację i praworządność. Organizatorzy: Rada Europy oraz Fińska Prezydencja Komitetu Ministrów RE.	Helsinki
18.	11-13.03.2019	8. posiedzenie plenarne Europejskiej Rady Ochrony Danych (EROD).	Bruksela
19.	18-20.03.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
20.	19-22.03.2019	47. Spotkanie Biura Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (T-PD Bureau).	Paryż
21.	20-22.03.2019	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela

22.	24-26.03.2019	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
23.	9-10.04.2019	9. posiedzenie plenarne Europejskiej Rady Ochrony Danych (EROD).	Bruksela
24.	3-4.05.2019	Dzień Otwarty instytucji UE (EU Open Days 2019).	Bruksela
25.	6.05.2019	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH) Europejskiej Rady Ochrony Danych.	Bruksela
26.	7.05.2019	Posiedzenie Grupy Koordynującej Nadzór nad Systemem Informacji Celnej (CIS).	Bruksela
27.	8-10.05.2019	29. Konferencja Europejskich Organów Ochrony Danych. Organizator: Biuro Inspektora Ochrony Danych Osobowych Gruzji.	Tbilisi
28.	10-12.05.2019	Warsztaty BCR	Oslo
29.	13-15.05.2019	10. posiedzenie plenarne Europejskiej Rady Ochrony Danych (EROD).	Bruksela
30.	13-16.05.2019	Wizyta studyjna w Centrum Legislacji i Badań Prawnych Białorusi	Strasburg
31.	13-17.05.2019	Krótkie programy szkoleniowe dla pracowników w ramach eOpenSpace projekt Erasmus+. Organizator: CPDP w Bułgarii.	Sofia
32.	21-22.05.2019	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
33.	21-22.05.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
34.	23.05.2019	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
35.	4.06.2019	11. posiedzenie plenarne Europejskiej Rady Ochrony Danych (EROD).	Bruksela
36.	11.06.2019	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
37.	11-12.06.2019	Warsztaty BCR.	Oslo
38.	13-14.06.2019	38. Posiedzenie plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD).	Strasburg
39.	18-19.06.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
40.	18-20.06.2019	Posiedzenie Podgrup: Granic, Podróży i Egzekwowania Prawa (BTLE), Grupy koordynującej nadzór nad Systemem Informacji Schengen drugiej generacji (SIS II), Eurodac, Grupy koordynującej nadzór nad Wizowym Systemem Informacyjnym (VIS).	Bruksela
41.	19-20.06.2019	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
42.	20.06.2019	Posiedzenie Podgrupy ds. Nakładania Kar (Fining Task Force) Europejskiej Rady Ochrony Danych.	Bruksela
43.	24.06.2019	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH) Europejskiej Rady Ochrony Danych.	Bruksela
44.	9-10.07.2019	12. posiedzenie plenarne Europejskiej Rady Ochrony Danych – EROD.	Bruksela
45.	16.07.2019	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela

46.	17-18.07.2019	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
47.	10-11.09.2019	13. posiedzenie plenarne Europejskiej Rady Ochrony Danych - EROD.	Bruksela
48.	16.09.2019	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmental and Health - CEH) Europejskiej Rady Ochrony Danych.	Bruksela
49.	17-18.09.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
50.	17-19.09.2019	Konferencja IAPP - Data Protection Intensive.	Monachium
51.	19.09.2019	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Europejskiej Rady Ochrony Danych	Bruksela
52.	20.09.2019	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media) Europejskiej Rady Ochrony Danych.	Bruksela
53.	23.09.2019	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
54.	24-25.09.2019	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement Expert Subgroup) oraz Podgrupy ds. Współpracy (Cooperation Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
55.	24-27.09.2019	Posiedzenie Biura Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (T-PD Bureau).	Paryż
56.	26.09.2019	Posiedzenie Podgrupy ds. Nakładania Kar (Fining Task Force) Europejskiej Rady Ochrony Danych.	Bruksela
57.	7-9.10.2019	13. posiedzenie plenarne Europejskiej Rady Ochrony Danych – EROD.	Bruksela
58.	14.10.2019	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH) Europejskiej Rady Ochrony Danych.	Bruksela
59.	15-16.10.2019	Posiedzenie Podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
60.	16.10.2019	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
61.	21-24.10.2019	41. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności. Organizator: Biuro Komisarza ds. Informacji i Ochrony Danych Albanii.	Tirana
62.	23-24.10.2019	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
63.	24.10.2019	Spotkanie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Europejskiej Rady Ochrony Danych.	Bruksela
64.	3-4.11.2019	Spotkanie interesariuszy dotyczące praw osób, których dane dotyczą.	Bruksela
65.	12-13.11.2019	15. posiedzenie plenarne Europejskiej Rady Ochrony Danych – EROD.	Bruksela
66.	13-16.11.2019	III Spotkanie partnerów Projektu „T4DATA" oraz konferencja kończąca Projekt. Organizator: Fundacja Fondazione Basso.	Rzym
67.	18.11.2019	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
68.	19-21.11.2019	39. posiedzenie plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych - T-PD.	Strasburg
69.	20.11.2019	Posiedzenie Podgrupy Technologii (Technology Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela

70.	20-21.11.2019	Podgrupy ds. Współpracy (Cooperation Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
71.	24-29.11.2019	Misja ewaluacyjna Schengen.	Nikozja
72.	25-26.11.2019	Konferencja z zakresu ochrony danych osobowych dla MŚP pt. „Dane mają wartość – chroń je!". Organizator Inspektorat Ochrony Danych Republiki Łotwy.	Ryga
73.	26-28.11.2019	Posiedzenie Podgrupy SIS, VIS, Eurodac, Europol.	Bruksela
74.	27.11.2019	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media) Europejskiej Rady Ochrony Danych.	Bruksela
75.	28-29.11.2019	Europejskie Warsztaty Rozpatrywania Spraw.	Bruksela
76.	2-3.12.2019	16. posiedzenie plenarne Europejskiej Rady Ochrony Danych – EROD.	Bruksela
77.	9-12.12.2019	33. Międzynarodowa Konferencja Czerwonego Krzyża i Czerwonego Półksiężyca. Organizator: Międzynarodowy Ruch Czerwonego Krzyża i Czerwonego Półksiężyca.	Genewa

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
www.uodo.gov.pl